Law, technology, and shifting power relations

Koops, E.J.

Published in:
Berkeley Technology Law Journal

Publication date:
2010

Document Version
Peer reviewed version

Citation for published version (APA):
Koops, E. J. (2010). Law, technology, and shifting power relations. *Berkeley Technology Law Journal*, *25*(2), 973-1035.

LAW, TECHNOLOGY, AND SHIFTING POWER RELATIONS

Bert-Jaap Koops[†]

> "I thought he was going to get pneumonia, but actually he said in his letter it wasn't the cold that bothered him, it was being watched all the time. The eye in the door." . . . This eye, where no eye should have been, was deeply disturbing to Prior. . . . "That's horrible," he said, turning back to Beattie. " 'S not so bad long as it stays in the door." She tapped the side of her head. "You start worrying when it gets in here."[1]

TABLE OF CONTENTS

---

† Professor of Regulation & Technology, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands. MSc (mathematics) and MA (literature), Groningen University, PhD (law), Tilburg University. The research for this Article was funded by the Netherlands Organisation for Scientific Research (NWO), whom I thank for its generous support. This Article presents the conclusions of a five-year project on law, technology, and shifting balances of power; it builds on the results of subprojects and hence will refer relatively frequently to earlier publications by me and my co-researchers in the project, Dr. Colette Cuijpers and Dr. Merel Prinsen.

1. PAT BARKER, THE EYE IN THE DOOR 36 (Plume 1995) (1993).

I. INTRODUCTION

Law and power are closely connected. In a lawless society, power will reign supreme, while in a society of rule of law, power is reined in by the law. However, law also establishes and validates power. The dual face of law—establishing and restraining power—is particularly relevant in unequal power relations, where the law both consolidates the power of strong parties and restricts their power by providing the weak parties with rights, in order to prevent them from being subjected to exercises of brute power. In this respect, inequality compensation is a key legal mechanism to regulate power relations. The law treats certain categories of people, including citizens, criminal suspects, employees, and consumers, as systematically weak parties relative to parties that are considered strong, such as the government, employers, and businesses. To balance these unequal power relationships weak parties are granted various rights in the domains of constitutional, administrative, labor, contract, and tort law. Examples include information rights, benefit-of-the-doubt and burden-of-proof rules, access to justice, and compensational rights.

This classic account of inequality compensation in legal domains is challenged by technology. With the advent of computers, the Internet, genetic profiling, and other information-related technologies, power relations

start to shift. Since "knowledge is power," as the adage holds, both strong and weak parties use information-related technologies to improve their respective information positions. For example, consumers can now use the Internet to search for the lowest prices and can use ratings websites to inform one another of their experiences with particular products and services. Such practices free the consumer from the monopoly power of the shop around the corner. However, the gain in power that technology has provided to consumers is paralleled by the gains that technology provides to businesses. For instance, technology enables e-businesses to gather more information about consumers—using cookies, web forms, and profiling techniques—than the classic brick-and-mortar shop. They can then use this information to target consumers with increasing sophistication.

The gross outcome of such shifts in power relations is unclear: changes occur in different directions and sometimes along different dimensions. Parties may become stronger in one way, weaker in another, or both, depending on the circumstances. These shifts in power along different axes complicate the traditional ex ante model of inequality compensation which is based on the idea that certain parties are intrinsically stronger than others and must always be restrained by legal norms.

This Article aims, first, to explore the technology-related shifts in power relations that are occurring in the domains of law enforcement, labor, and commerce. Second, it aims to identify and examine the consequences of these shifts for the legal protection of weak parties, particularly for existing mechanisms of inequality compensation in the associated legal domains.

The domains of law enforcement, labor, and commerce exemplify unequal power relations and together cover a wide range of public and private law. Furthermore, technology is associated with significant shifts in the ways in which power is exercised today in these domains. Although the mechanism of inequality compensation will occur in most modern legal systems, the analysis is limited to the legal systems of the United States and the Netherlands and the concrete examples of legal protection that they supply.[2] The Article will explore these countries, with their different common law and civil law traditions, in a roughly comparative approach to discover differences and commonalities in the compensation granted to weak parties for inequalities in power relations.

2. Where Dutch law is based on European Union (E.U.) law, I will focus on the E.U. law. I will also occasionally mention developments in U.K. law where these are illustrative, particularly in the area of criminal law.

After some preliminaries in Part II that further introduce the notions of power relations, inequality compensation, and technology, the Article examines the relationship between law enforcement and citizens in Part III, employers and employees in Part IV, and businesses and consumers in Part V. The analysis is grounded in case studies to illustrate the effect of information-related technologies on shifting power relations. These case studies form the basis for a more general discussion of shifts in the power relation and their consequences for legal protection of weak parties. Then, Part VI provides an integrated view of citizens, employees, and consumers and the way in which the different roles of individuals are becoming intertwined in the information society. This forms the basis for drawing some conclusions in Part VII, not only about the distinct areas of law for specific categories of people, but also about the overall legal protection of individuals in the information society.

II. PRELIMINARIES

A. POWER RELATIONS

Power is complex and multifaceted. The term "power" comprises a wide array of notions bearing Wittgensteinian family resemblances.[3] It even comes close to being an "essentially contested concept," that is, a concept "the proper use of which inevitably involves endless disputes about their proper uses on the part of their users."[4]

For the purposes of this Article, the working definition of power is drawn from Dahl's conceptualization of power relations: "A has power over B to the extent that he can get B to do something that B would not otherwise do."[5] This definition shows exactly why weak parties are given legal

3. The many notions of power are connected by a series of overlapping similarities, but no one feature is common to all. For an introduction into the concept of "family resemblances," see generally LUDWIG WITTGENSTEIN, PHILOSOPHICAL INVESTIGATIONS (P.M.S. Hacker & Joachim Schulte eds., G.E.M. Anscombe et al. trans., Blackwell Publishing Ltd. 2009) (1953).

4. W. B. Gallie, *Essentially Contested Concepts*, 56 PROC. ARISTOTELIAN SOC'Y 167, 169 (1956); *see also* Eugene Garver, *Rhetoric and Essentially Contested Arguments*, 11 PHIL. & RHETORIC 156 (1978) (connecting Gallie's essentially contested concepts to Aristotle's account of rhetorical argument). For overviews of the many notions of power, see generally MARK HAUGAARD, POWER: A READER (2002) and JOHN SCOTT, POWER (2001). It is not possible to discuss the concept itself in this Article. Fortunately, there is no need to; since this Article looks at power relations from the perspective of legal protection of weak parties against strong parties, it suffices to provide a working definition that fits in this context. The Article, after all, aims to reflect on legal protection of weak parties rather than on power relations per se.

5. Robert A. Dahl, *The Concept of Power*, 2 BEHAV. SCI. 201, 202–03 (1957); Robert A.

protection in power relations. From the perspective of autonomy—a key value underlying modern Western legal systems—B should be able to decide without undue restrictions what she wants to do, and not merely because A makes her do so.

This working definition can be enriched with some insights that refine Dahl's conceptualization. Bachrach and Baratz have called attention to a second dimension of power by pointing out that power can be exercised indirectly and passively by limiting the scope of decision-making to exclude issues of relevance to B, for example, by (non-)agenda setting.[6] Lukes has added a third dimension, namely, the bias in a system sustained "by the socially structured and culturally patterned behaviour of groups, and practices of institutions."[7] Foucault has provided an important variation of Lukes' third dimension with his insights into the power mechanism of surveillance architecture. This is famously illustrated by the Panopticon, a mechanism where watched people (prisoners) aware of the continuous gaze of the watcher (the prison guard) internalize the value and knowledge system of the watcher, disciplining themselves according to the dominant discourse in society.[8]

This Article studies power relations in which A can get B to do something which B would not otherwise do, with a broad interpretation of "getting to do" that includes non-decision-making as well as cultural, institutional, and architectural mechanisms that have a disciplining effect on B.

B. LEGAL PROTECTION: INEQUALITY COMPENSATION

The legal phenomenon of inequality compensation that is embedded in the law is based on the idea that in society there are specific parties that have a structural, systematic advantage over other specific parties. This was a

---

Dahl, *Power*, *in* INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL SCIENCES (David L. Sills ed., 1968).

6. Peter Bachrach & Morton S. Baratz, *Two Faces of Power*, 56 AM. POL. SCI. REV. 947, 948 (1962).

7. *See generally* STEVEN LUKES, POWER: A RADICAL VIEW 26 (2005) (1974). Note, however, Haugaard's critique, HAUGAARD, *supra* note 4, at 38–40, that Lukes' stress on socially constituted bias makes it difficult to distinguish power from structural constraint. Haugaard suggests that an integrated theory of power and structure needs to be developed. *Id.*

8. For a critical discussion of panopticism, see generally David Lyon, THEORIZING SURVEILLANCE: THE PANOPTICON AND BEYOND (Devon Cullompton ed., 2006). *See also* MICHAEL FOUCAULT, POWER: ESSENTIAL WORKS OF FOUCAULT 1954–1984 (James D. Faubion ed., 2000); MICHEL FOUCAULT, SURVEILLER ET PUNIR: NAISSANCE DE LA PRISON (1975).

natural and valid assumption to make when the current systems were shaped during the nineteenth and most of the twentieth century. The relationship between law enforcement and citizens, between employers and employees, and between enterprises and consumers was by and large clear: the former could easily impose their will on the latter, unless something—such as legal norms—prevented or corrected them.

It is an important function of the law to compensate for such structural inequalities. Criminal, consumer, and labor law have developed to regulate structural imbalances by protecting the weak party against abuse of power by the strong party. The protection takes the form of inequality compensation which imposes duties on strong parties and grants rights to weak parties. Examples include rights related to information provision, notification duties, supervision mechanisms, and access to justice. The legal system views citizens, employees, and consumers as intrinsically disadvantaged parties that require structural inequality compensation. These legal-protection rules are triggered by the mere fact of belonging to the class of the weak party at issue, irrespective of the specific manifestation of the power relation in concrete circumstances.

C. TECHNOLOGY

In a society as complex as the modern information and network society,[9] it may no longer be valid to assume that traditionally dominant parties remain more powerful than other parties. Partly through the influence of new technologies, most notably information and communication technology (ICT), but also genetic and surveillance technologies, unequal relationships seem to be shifting. This happens in subtle and often contradictory ways. Parties that were once considered weak by the very nature of the power relationship may emerge as the stronger party in certain circumstances. Alternatively, they can find themselves even weaker than they were before.

Technology plays a significant role in these shifts. For instance, increasingly sophisticated technology enables criminals to protect their communications from police surveillance and store incriminating electronic evidence in a data haven abroad, outside the reach of mutual legal assistance. However, technology also facilitates criminal investigation by supplying unprecedented surveillance tools, such as, microscopic sensors, smart cameras, and keyboard sniffers (i.e., software that secretly records keystrokes and sends these to the police). In the field of commerce, e-businesses can collect much more data about customers using technology such as cookies

9. *See generally* MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY (Blackwell, 1996) (charting the social and economic relations of the global information economy).

and loyalty schemes. Consequently, these businesses are in a better position than ever to exploit their information advantage over the customer. At the same time, e-consumers can search the web for the lowest prices, participate in collective-buying activities, and set up grudge websites[10] to force a company to change its policy.

Admittedly, the role of technology in shifts in power relations is not always clear or easy to isolate from other factors. After all, power relations develop in social, economic, cultural, political, and architectural contexts. Technology is sometimes a sufficient cause for a certain development, sometimes a necessary cause, sometimes both, and at other times neither. Technological developments interact with other societal developments, in a process of mutual shaping where both developments influence each other.[11]

This Article does not aim to determine the causal influence of technology on power relations as such; rather, it limits its inquiry to describing shifts in power relations in which technology plays some role. This includes circumstances where technology opens up new possibilities for a strong party to exercise power, where it creates new opportunities for weak parties to resist the power of a strong party, or even where it blurs the very distinction between a strong and a weak party.

Because power relations hinge on knowledge and information[12] it will be important to examine information technologies. However, while the case studies in this Article primarily involve ICT, technologies relating to genetic information have also contributed to technology-related shifts in power relations, particularly through the advent of DNA forensics.

III. LAW ENFORCEMENT–CITIZEN

This Part examines technology-related changes in the power relation of law enforcement and citizens, and assesses the consequences of these changes for the legal protection of citizens. The analysis begins with three case studies: DNA forensics, interception of telecommunications, and

10. *See, e.g.*, Wakeup Walmart.com: America's Campaign to Change Wal-Mart, http://www.wakeupwalmart.com (last visited Apr. 4, 2010).

11. For example, the introduction of mobile telephones has significantly changed the way people communicate. Specifically, mobile telephone users started using the SMS function of mobile telephones on a large scale and in ways completely unforeseen by its developers, thereby changing the technology. For a discussion of the mutual shaping of technology and society, see SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE (Wiebe E. Bijker & John Law eds., 1992).

12. *See* FOUCAULT, POWER, supra note 8, at 133 (arguing that power hinges on the political, economic, and institutional regime of the production of truth).

Passenger Name Records. Based on these case studies, a general discussion follows, outlining major developments and showing that the government, in its role as the protector of law and order, has embraced the enormous increase in technology-enabled tracing capacity. This development has not been offset by counter-developments of citizen empowerment. The resulting shift in power relation involves two types of problems—citizens being wrongly involved in a government investigation and a potentially disciplining effect of surveillance architectures—which seem to require new forms of legal protection.

A. CASE STUDY 1: DNA FORENSICS

Since the invention of DNA fingerprinting in the 1980s, DNA forensics have contributed to a gradual expansion in investigation powers.[13] Different types of DNA research have been developed and used in criminal investigation including DNA databasing, DNA phenotyping, mass screening, and familial searching.

The rise of DNA databasing is most visible in England and Wales, where the U.K. database, National DNA Database (NDNAD), has expanded enormously over the past decade. In 2007, it contained up to four million profiles (around six percent of the population), which were gathered through routine sampling and profile retention from arrestees as well as victims, consenting witnesses, and volunteers.[14] The U.S. national database, Combined DNA Index System (CODIS), was originally smaller in size, but outgrew the U.K. database in 2007, with 4.6 million profiles (around 1.5

13. *See generally* NUFFIELD COUNCIL ON BIOETHICS, THE FORENSIC USE OF BIOINFORMATION: ETHICAL ISSUES (2007) (examining the balance between police powers and individual rights to autonomy and privacy and offering recommendations to minimize misuses); MEREL M. PRINSEN, FORENSISCH DNA-ONDERZOEK: EEN BALANS TUSSEN OPSPORING EN FUNDAMENTELE RECHTEN (2008) (critically assessing Dutch and U.K. approaches to forensic DNA legislation); ROBIN WILLIAMS ET AL., GENETIC INFORMATION AND CRIME INVESTIGATION: SOCIAL, ETHICAL AND PUBLIC POLICY ASPECTS OF THE ESTABLISHMENT, EXPANSION AND POLICE USE OF THE NATIONAL DNA DATABASE (2004) (discussing the evolution in the use of genetic information in criminal investigations from case-by-case use to extensive and routine practice).

14. NUFFIELD COUNCIL ON BIOETHICS, *supra* note 13, at 9. Note that the current English and Welsh practice of retaining profiles and samples from unconvicted offenders should be changed in light of the European Court of Human Rights' judgment in *S. and Marper v. United Kingdom*, 2008 Eur. Ct. H.R. 1581; *see* HOME OFFICE, KEEPING THE RIGHT PEOPLE ON THE DNA DATABASE: SCIENCE AND PUBLIC PROTECTION (2009) (reporting on the government's consultation process launched in May 2009). The proposed "change" comprises retention of profiles from unconvicted people for six years for less serious crimes or twelve years for serious crimes, which does not seriously alter the policy of storing data from non-criminal citizens.

percent of the population).[15] In addition to CODIS, DNA databases exist in the United States at state and local levels, often containing more profiles. U.S. states are continually expanding their databases, allowing DNA samples to be taken from convicts and profiles to be stored for an increasing variety of crimes as well as for groups of citizens charged but not convicted.[16]

In the Netherlands, the power to take a DNA sample from a suspect was introduced in 1994, and then expanded in 2001 to allow for DNA collection in more types of crime and without a magistrate's warrant. In 2004, the DNA Convict Sampling Act allowed the Public Prosecutor to take samples from convicts in the interest of deterrence and to ensure more future matches with repeat offenders.[17] The Dutch database is smaller than the U.K. and U.S. databases; nevertheless, since the 2004 Act it has exploded, growing from 6,000 individual profiles in early 2005, to 45,000 in December 2007, to over 99,000 (around 0.6 percent of the population) in May 2010.[18]

As the use of DNA forensics has become more common, new qualitative methods of DNA analysis have also developed. For example, forensic DNA phenotyping, a relatively recent development, uses personal characteristics determined from crime scene DNA to trace unknown suspects.[19] This can help limit the pool of possible suspects so that law enforcement officials can conduct a mass-screening investigation. Alternatively, it can help exclude certain groups of people from further investigation. In England and Wales, the Forensic Science Service can determine the rough geographical ancestry of the DNA sample donor,[20] and at one time it offered a service to check for

15. NUFFIELD COUNCIL ON BIOETHICS, *supra* note 13, at 9.

16. *See generally* Aaron P. Stevens, *Arresting Crime: Expanding the Scope of DNA Databases in America*, 79 Tex. L. Rev. 921 (2001) (describing the history of DNA databases and their expansion to include more classes of criminals); Bonnie L. Taylor, *Storing DNA Samples of Non-Convicted Persons & the Debate over DNA Database Expansion*, 20 T.M. Cooley L. Rev. 509 (2003) (arguing that the national trend of expanding DNA databases to include more unconvicted individuals violates the Fourth Amendment and privacy rights).

17. Wet DNA-onderzoek in strafzaken, Staatsblad van het Koninkrijk der Nederlanden [Stb.] 596 (1993) (Neth.); Wet van 5 juli 2001 tot wijziging van de regeling van het DNA-onderzoek in strafzaken, Staatsblad van het Koninkrijk der Nederlanden [Stb.] 335 (2001) (Neth.); Wet DNA-onderzoek bij veroordeelden, Staatsblad van het Koninkrijk der Nederlanden [Stb.] 465 (2004) (Neth.).

18. DNA: Sporen Naar de Toekomst, http://www.dnasporen.nl (last visited July 1, 2010). See also the comparison of U.K. and Dutch developments in PRINSEN, *supra* note 13.

19. For technical and regulatory discussions see Bert-Jaap Koops & Maurice Schellekens, *Forensic DNA Phenotyping: Regulatory Issues*, 9 COLUM. SCI. & TECH. L. REV. 158 (2008); Pilar N. Ossorio, *About Face: Forensic Genetic Testing for Race and Visible Traits*, 34 J.L. MED. & ETHICS 277 (2006).

20. This is contested, first because individuals' DNA shows more variation than the variations of geographic groups of people, and second, because race is a social rather than a

red hair and light skin pigment.[21] Determining geographical ancestry or ethnic background is becoming more popular as scientific knowledge about DNA evolves.[22] As genetic knowledge advances, other phenotypical characteristics, such as hair, form, or height, may become available. In common law systems, such as those in the United States and the United Kingdom, use of a new technology is allowed until legislation or case law dictates otherwise.[23] In contrast, in civil law systems, new investigation techniques can usually only be used when legislation specifically allows it. The Netherlands, for example, enacted a law allowing phenotyping for geographic ancestry and gender. Other features, such as hair color, however, must be designated by an Order in Council (i.e., a lower-order regulation based on the statute) before the police can derive them.[24]

A third development is the use of DNA mass screening, or dragnet investigations, in which a group of people who match a suspect description are asked to voluntarily provide a DNA sample for profiling. This method was first used in the United States in 1990, when over 800 men in San Diego were tested in connection with a sextuple murder, and it has been used many times since.[25] Dragnet investigations have raised constitutional concerns where the volunteers' consent to DNA testing was given under police coercion. A paradigmatic example would be when a police officer gives an

---

genetic concept. *See* NUFFIELD COUNCIL ON BIOETHICS, *supra* note 13, at 80–81.

21. FORENSIC SCIENCE SERVICE, FACT SHEET: COMMONPLACE CHARACTERISTICS (2004), *available at* http://www.forensic.gov.uk. This service was discontinued due to insufficient demand from the police. For recent technological developments in deriving visible traits from crime-scene DNA, see Manfred Kayser & Peter M. Schneider, *DNA-Based Prediction of Human Externally Visible Characteristics in Forensics: Motivations, Scientific Challenges, and Ethical Considerations*, 3 FORENSIC SCI. INT'L: GENETICS 154 (2009); Fan Liu et al., *Eye Color and the Prediction of Complex Phenotypes from Genotypes*, 19 CURRENT BIOLOGY 192 (2009).

22. *See* Mark D. Schriver & Rick A. Kittles, *Genetic Ancestry and the Search for Personalized Genetic Histories*, 5 NATURE REVS. GENETICS 611 (2004).

23. *See* Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 791–92 (1999); Koops & Schellekens, *supra* note 19, at 27–32. In the United States, only Indiana, Rhode Island, and Wyoming have outlawed forensic phenotyping. *See* IND. CODE ANN. § 10-13-6-16 (West 2004); R.I. GEN. LAWS § 12-1.5-10 (2007); WYO. STAT. ANN. § 7-19-404 (2007).

24. Wet van 8 mei 2003 tot wijziging van de regeling van het DNA-onderzoek in strafzaken in verband met het vaststellen van uiterlijk waarneembare persoonskenmerken uit celmateriaal [Act of May 8, 2003], Staatsblad van het Koninkrijk der Nederlanden [Stb.] 201 (2003) (Neth.).

25. Philip P. Pan, *Pr. George's Chief Has Used Serial Testing Before; Farrell Oversaw DNA Sampling of 2,300 in Fla.*, WASH. POST, Jan. 31, 1998, at B1 ("One of the first agencies to experiment with the [DNA dragnet] was the San Diego police department, which tested about 800 men during its search for a serial killer who stabbed six women to death in their homes between January and September 1990.").

individual the "choice" between providing a sample voluntarily or being subjected to a court order for DNA testing and enduring the publicity that such an order would generate.[26]

The Netherlands has also used DNA mass screenings in a score of cases, starting with the 1999 testing of 115 men in the still unsolved case of a serial rapist in Utrecht.[27] Between 1999 and 2004, approximately 4,600 people were asked to volunteer a DNA sample in fourteen cases.[28] The Dutch practice has to conform to policy criteria—provided by the Minister of Justice—that favor restricted use. These are generally reserved for the most serious crimes that cause significant social unrest,[29] and must be made with authorization from the Board of Procurators-General, the highest body within the Public Prosecutor. In 2007, the policy was expanded. Mass screening is no longer a tool of last resort, but rather part of the reasonable effort extolled by law enforcement during investigations.[30]

The fourth, and final recent innovation in DNA forensics is familial searching. This involves searching a database for partial matches of DNA profiles that suggest that the unknown person who left the stain at the crime scene is closely related to a known person whose DNA is stored in the DNA database. Familial searching was first used in England in 2002 in solving a 1973 double homicide case.[31] The crime scene stains had been profiled with Low Copy Number analysis, a new technique so sensitive that it can yield a DNA profile from only a few body cells, and yielded a partial match with a profile in the database.[32] Ultimately the father of the partial match, then deceased, was identified as the perpetrator.[33]

---

26. *See* Sepideh Esmaili, *Searching for a Needle in a Haystack: The Constitutionality of Police DNA Dragnets*, 82 CHI. KENT L. REV. 495 (2007).

27. CHRISTIANNE J. DE POOT & EDWIN W. KRUISBERGEN, KRINGEN ROND DE DADER GROOTSCHALIG DNA-ONDERZOEK ALS INSTRUMENT IN DE OPSPORING [CIRCLES AROUND THE PERPETRATOR: LARGE-SCALE DNA-ANALYSIS AS A TOOL IN CRIMINAL INVESTIGATION] 33 (2006).

28. *Id.* at 203.

29. Kamerstukken II, 2000-2001, 27 400 VI, No. 49 (Neth.).

30. Kamerstukken II, 2007-2008, 34 415, No. 1 (Neth.).

31. Robin Williams & Paul Johnson, *Inclusiveness, Effectiveness and Intrusiveness: Issues in the Developing Uses of DNA Profiling in Support of Criminal Investigations*, 33 J.L. MED. ETHICS 545, 554 (2005); Robin McKie, *Did a Killer Evade Justice Due to Withheld Evidence? The Collapse of the Case Against Angus Sinclair was a Bitter Blow to a Scientist Whose DNA work was not Fully Presented in Court*, THE OBSERVER, Sept. 16, 2007, at 17.

32. Williams & Johnson, *supra* note 31, at 554.

33. *Id.* In the Netherlands, familial searching requires a statutory basis which does not yet exist, but which has been proposed by the government. Kamerstukken II, 2007-08, 34 415, No. 1 (Neth.); *see also* Merel M. Prinsen, *DNA-verwantschapsonderzoek. Familie van de verdachte?*, 6 STRAFBLAD 242 (2008) (discussing pros and cons of familial searching in the

Familial searching provides an interesting expansion of policing, since it "effectively increases police scrutiny and interest in people based on their relatives' past involvement with the criminal justice system."[34] This practice raises three main concerns. First, it could have "differential effects on groups in American society."[35] Second, it raises questions about whether the consent given by volunteers in a mass screening is truly informed. That is, are volunteers sufficiently informed that permitting their DNA to be included in a forensic database can also affect their relatives? Finally, familial searching unearths ethical concerns in situations where individuals are not aware that their social family is not their biological family, for example, when the assumed father turns out not to be the biological father.[36]

B. CASE STUDY 2: INTERCEPTION OF TELECOMMUNICATIONS

Over the past decades, interception of communications has expanded greatly in the United States and, particularly, in the Netherlands. In the United States, interception of phone (wire) communications was regulated[37] after *Katz* interpreted the Fourth Amendment to protect telephone communications.[38] In 1986, the Electronic Communications and Privacy Act (ECPA) enabled the interception of electronic communications under less strict conditions than those that govern wire interception.[39] ECPA also allowed wiretapping for more types of crimes and introduced "roving" interception, which involves following the targeted suspect rather than focusing on fixed phone lines or places.[40] The USA Patriot Act of 2001 allowed interception for even more crimes, and it transferred voice mail from

---

Dutch context).

34. Henry T. Greely et al., *Family Ties: The Use of DNA Offender Databases To Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248, 255 (2006).

35. *Id.*

36. *See* Williams & Johnson, *supra* note 31, at 554–56 (assessing the effects of the recent innovative use of DNA databasing for "familial searching" and the way it has unsettled agreed understandings about appropriate uses of DNA). *See generally* Erica Haimes, *Social and Ethical Issues in the Use of Familial Searching in Forensic Investigations: Insights from Family and Kinship Studies*, 34 J.L. MED. & ETHICS 263 (2006) (exploring the socio-ethical concerns raised by familial searching of forensic databases in criminal investigations).

37. Omnibus Crime Control and Safe Streets Act, 18 U.S.C. § 2510 (2006).

38. *See* Katz v. United States, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

39. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. § 2510 (2006)).

40. *Id.*

the wiretap regime to the less protected communications storage regime.[41] The Netherlands experienced similar expansion.[42] Particularly significant was the Special Investigation Powers Act of 2000 that broadened the scope of police powers to allow interception of the connection not only of suspects, but also of non-suspects, provided that such interception could benefit the investigation.[43]

While the law in the books broadened over time, an equally important expansion of interception powers occurred in practice. In the United States, the number of interception authorizations (for criminal investigation, not for intelligence or national security) tripled since 1987 (from 673 authorizations in 1987 to 1,891 in 2008), and the average number of intercepted communications in each case doubled (from 1,299 communications in 1987 to 2,707 in 2008), so that the total amount of communications intercepted sextupled.[44] In the Netherlands, the available figures are much higher: in 1993, 3,619 interception authorizations were granted for criminal investigation (more, in absolute terms, than in the United States),[45] rising to 10,000 in 1999, and 26,425 authorizations in 2008.[46] This does not mean that over a decade, ten times more people have been under wiretap. Authorizations are given for separate connections, such as fixed and mobile phones, and criminals today have substantially more phones; nevertheless, the trend is undeniably upwards. Furthermore, given the enormous increase

41. Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

42. *See generally* ARNO HUBERTUS HENRICUS SMITS, STRAFVORDERLIJK ONDERZOEK VAN TELECOMMUNICATIE (2006) (surveying the historical development of Dutch law in the area of criminal investigation of telecommunications).

43. *See* WETBOEK VAN STRAFVORDERING [CRIM. PROC. CODE] art. 126n, 126u, introduced by the Wet bijzondere opsporingsbevoegdheden [Special Investigatory Powers Act], Staatsblad van het Koninkrijk der Nederlanden [Stb.] (1999) 245 (Neth.).

44. ADMIN. OFFICE OF THE U.S. COURTS, 2008 WIRETAP REPORT 7 (2008), *available at* http://www.uscourts.gov/wiretap08/contents.html [hereinafter 2008 WIRETAP REPORT]; ADMIN. OFFICE OF THE U.S. COURTS, 1997 WIRETAP REPORT 30 (1999), *available at* http://www.uscourts.gov/wiretap/contents.html. Note, however, a slight decrease in recent years: the 2007 numbers were higher, with 2,208 authorizations and 3,106 intercepts on average. 2008 WIRETAP REPORT, *supra*, at 32.

45. Wiretapping for intelligence versus criminal investigation purposes may yield a quite different picture, although it is difficult to compare these due to the official secrecy associated with intelligence practice.

46. The 1993 figure is from Z. REIJNE, TAPPEN IN NEDERLAND (1996). The 2000 figure is mentioned in Grootschalig afluisteren van moderne telecommunicatiesystemen, Kamerstukken II, 2000-2001, 27 591, No. 2. The 2008 figure is given in Kamerstukken II, 2009-2010, 30 517, No. 13 (Neth.)—the first annual systematic Dutch wiretap figures to be officially published.

in communications generally, particularly since the advent of mobile phones with short message service (SMS) capability and the Internet, much more data have become available to the police through intercepts. This is not only a quantitative increase, but also a qualitative increase. New types of data, such as internet browsing and location data, now allow long distance glimpses of human life that were previously hidden to the police, or observable only with significant effort and costs.

Another development has occurred in interception: the introduction of mandatory interceptability. Until the early 1990s telephone communications were easily interceptable. Then, because of an increase in market parties and diversification of telecom technologies, the police began to encounter difficulty intercepting. Concerned that a major investigation tool might be lost, governments passed laws forcing telecommunication providers to build in interceptability. The U.S. Communications Assistance for Law Enforcement Act (CALEA) of 1994[47] and Chapter 13 of the Dutch Telecommunications Act of 1998 imposed obligations on telecommunications carriers to ensure interceptability.[48] A statement by Dutch Member of Parliament highlights the reasoning behind these laws: "The traditional form of telephony can be intercepted. An alternative must be the same. We find that being interceptable is an *inseparable* part of the phenomenon of telephony in our country."[49]

---

47. Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1008(b)(1) (2006); *see also* AskCALEA: Communications Assistance for Law Enforcement Act, http://www.askcalea.net (last visited Jan. 31, 2010) (acting as a resource and information clearinghouse for individuals and organizations with an interest in the Communications Assistance for Legal Enforcement Act of 1994).

48. Telecommunicatiewet [Telecommunications Act], Staatsblad van het Koninkrijk der Nederlanden [Stb.] 610 (1998) (Neth.); *see also* Council Resolution 96/C329/01, 1996 O.J. (C 329) 1 (EC) (addressing the lawful interception of telecommunications). For a comparison of the U.S. and Dutch legislation, which shows a more liberal approach to impositions on market parties in the United States, see Bert-Jaap Koops & Rudi Bekkers, *Interceptability of Telecommunications: Is US and Dutch Law Prepared for the Future?*, 31 TELECOMM. POL'Y 45 (2007). This analysis shows that the U.S. approach, as laid down in CALEA, is essentially more flexible and balanced than the Dutch approach. CALEA already presumes some form of trade-off, through the crucial provision of 47 USC § 1008(b)(1), which lists ten factors to be taken into account in determining the reasonableness of requiring a particular telecom provider to build in interceptability, is flanked by several other checks and balances that ensure enhanced cost-effectiveness. The authors conclude that the rigid Dutch law cannot handle such a trade-off since it requires tout court that new telecommunications networks and services are made interceptable and that the providers fund these measures, regardless of the costs or the effects on security, privacy, or innovation.

49. Handelingen II, Oct. 25, 1995, 17-1123 (Neth.) (translation by Bert-Jaap Koops, emphasis added). In a related development, when technologists discovered that cell telephones were capable of "knowing" their location, governments started to mandate that

C. CASE STUDY 3: PASSENGER NAME RECORDS[50]

Apart from developments in regular criminal investigation discussed in the previous case studies, anti-terrorism developments in the periphery of criminal law also merit attention. In this area, the mandatory exchange between countries of Passenger Name Records (PNR) of air travelers constitutes an interesting case study. PNR include information such as a passenger's name and address, birth date, passport details, payment data, emergency contacts, and meal and seating preferences. After the 9/11 terrorist attacks on New York and Washington, D.C., in 2001, the United States believed that processing PNR might help to keep terrorists out of the country. The Bureau of Customs and Border Protection (CBP) started asking airlines to provide the government with access to their PNR records. For European airlines, this processing of personal data for purposes other than the original purposes for which the data were collected violated data protection legislation if conducted without a legal ground. Consequently, the European Union (E.U.) made an agreement with the United States to authorize the provision of PNR.[51] The agreement did not authorize the *exchange* of PNR data, but only the one-way access of U.S. government agencies to European data.

The PNR agreement, however, was controversial. The European Parliament felt that it had been outmaneuvered as protector of the privacy of European citizens and challenged the underlying documents[52] before the European Court of Justice. The Court struck down the Commission's and Council's decisions, finding that they were based on the wrong legal ground, and thereby effectively annulled the PNR agreement.[53] However, the

---

mobile phones be made with the ability to make their location known in case an emergency number was called. *See generally* David J. Phillips, *Privacy and Data Protection in the Workplace: The US Case*, *in* REASONABLE EXPECTATIONS OF PRIVACY? 39 (Sjaak Nouwt et al. eds., 2005) (concluding that although the impetus for these mandates was not crime-control but safety concerns, as a result locatability has become an inherent feature of mobile phones, and as a consequence, generated location data will routinely be available for criminal investigation purposes).

50. This Section builds on Vagelis Papakonstantinou & Paul De Hert, *The PNR Agreement and Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework on Either Side of the Atlantic*, 46 COMMON MKT. L. REV. 885 (2009).

51. On the European side, the agreement was backed up by two official documents: Commission Decision 2004/535, 2004 O.J. (L 235) 11 (EC), and Council Decision 2004/496, 2004 O.J. (L 183) 83 (EC).

52. *Id.*

53. Joined Cases C-317/04 & 318/04, Parliament v. Council, 2006 E.C.R. I-04721 (holding that the Agreement had been passed as a measure in the area of justice and home affairs (where the European Commission and European Council take decisions), while it should have been passed as a measure related to economic, social, and environmental

European Parliament's action backfired, by triggering a renegotiation with the United States on a second PNR agreement, in which the United States emerged even stronger.

The second PNR agreement was concluded on June 29, 2007 and memorialized in three documents.[54] It comprises fewer passenger records than the first agreement—nineteen instead of thirty four—but since the records contain the same types of information, only in a different format, this was only a cosmetic reduction. The records can be retained significantly longer than before—fifteen instead of three and a half years—and it is not guaranteed that the records will be destroyed after this period.[55] Moreover, a wider range of U.S. agencies, not only customs, can access the data, and the data may be transferred to other countries at the discretion of the U.S. Department of Homeland Security (DHS).[56]

Perhaps most importantly for our purposes, although the PNR Agreements were initiated in the post 9/11 wave of anti-terrorism measures, the PNR data may be used by the U.S. government for combating or preventing not only terrorism, but also

> other serious crimes, including organized crime, that are transnational in nature. PNR may be used where necessary for the protection of the vital interests of the data subject or other persons, or in any criminal judicial proceedings, or as otherwise required by law. DHS will advise the EU regarding the passage of any U.S. legislation which materially affects the statements made in this letter.[57]

In other words, personal data of European citizens collected to facilitate air travel accommodations are now mandatorily provided to the U.S. government in the interest of counter-terrorism, and can simultaneously be

---

policies (where the European Parliament has co-decision power alongside the Commission and Council)).

54. The three documents are (1) an agreement signed by both parties, (2) a U.S. letter to the E.U. assuring how it will handle European PNR data in the future, and (3) a letter from the E.U. to the United States acknowledging receipt of this letter. *See* Council Decision 2007/551/CFSP/JHA, 2007 O.J. (L 204) 16 (EU). The relationship between the three documents makes the agreement uncertain, thereby complicating the assessment of its exact legal status and contents. *See* Papakonstantinou & De Hert, *supra* note 50, at 908–19.

55. Papakonstantinou & De Hert, *supra* note 50, at 912 (citing Ch.VII, U.S. Letter to the European Union in Council Decision 2007/551, 2007 O.J. (L 204) 16–25 (EC)) ("We expect that EU PNR data shall be deleted at the end of this period; questions of whether and when to destroy PNR data collected in accordance with this letter will be addressed by DHS and the EU as part of future discussions.").

56. *Id.* at 911.

57. *Id.*

used for combating serious crime, protecting vital interests, or any other purposes currently or later stipulated by U.S. law. "Function creep" seems a bland description of this deviation from the principle of purpose specification and use limitation that is ingrained in European data protection law.[58] The rapid expansion of PNR functionality seems better captured by the term "function rush."

The developments in PNR are not solely products of U.S. political pressure. Several E.U. countries have also started to require access to PNR and store these data for anti-terrorism or other purposes, and a Framework Decision is being proposed to introduce PNR processing throughout the E.U.[59] Interestingly, air carriers already must communicate Advance Passenger Information (API) to authorities of E.U. Member States for fighting illegal immigration;[60] "[t]he added value of PNR is that it helps identify unknown people and develop risk indicators."[61] Some member states, including the United Kingdom, would like to see the purpose of PNR processing extended from fighting terrorism and organized crime to other purposes as well.[62]

D. DISCUSSION

Broad use of DNA forensics and interception of communications is representative of a wide range of advances in criminal investigation using new technologies or new applications of existing technologies. The means for searching computers, collecting traffic data, ordering the production of computer data, employing camera and olfactory surveillance,[63] and utilizing forensic chemistry have developed significantly over the past two decades.[64]

---

58. *See* Directive 95/46/EC, art. 6(1)(b), 1995 O.J. (L 281) 31 (EC).

59. Press Release, European Commission, Proposal for a COUNCIL FRAMEWORK DECISION on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes, Memo/07/449 (Nov. 6, 2007), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/449&format=HTML&aged=0&language=EN&guiLanguage=en.

60. Directive 2004/82/EC, 2004 O.J. (L 261) 24 (EU).

61. Press Release, European Commission, *supra* note 59.

62. *See* SEC'Y OF STATE FOR THE HOME DEP'T, THE PASSENGER NAME RECORD (PNR) FRAMEWORK DECISION: THE GOVERNMENT REPLY TO THE FIFTEENTH REPORT FROM THE HOUSE OF LORDS EUROPEAN UNION COMMITTEE SESSION 2007-08 HL PAPER 106, 1–2 (2008) (recommending that PNR be extended to "serious crimes").

63. Olfactory surveillance is conducted by detecting scents, for example, with sniffer dogs or wasps to detect drugs or chemicals. *See* Amber Marks, *Drug Detection Dogs and the Growth of Olfactory Surveillance: Beyond the Rule of Law?*, 4 SURVEILLANCE & SOC'Y 257 (2007) (discussing the expansion of olfactory surveillance in the United Kingdom through increased use of drug detection dogs and arguing that it sets a dangerous precedent for the regulation of other surveillance technologies).

64. *See* KRISTIE BALL ET AL., A REPORT ON THE SURVEILLANCE SOCIETY: FOR THE

The PNR case study, moreover, is emblematic of government anti-terrorism measures and efforts in the fringes of crime-fighting. This includes a host of administrative or pseudo-criminal measures—incorporating biometrics in travel documents, increased identification duties, preventative frisking, and scanning of laptops at customs—taken to scan and store data about groups of people to prevent potentially dangerous activities.

Evident in these case studies is a consistent pattern of increasing traces. Citizens leave digital traces when exploring the Internet, using automatic teller machines (ATMs) and point-of-sale terminals, entering secured buildings, walking the streets under the watchful eyes of closed circuit television (CCTV); they leave physical traces when walking around, touching objects, smoking cigarettes, combing their hair, or drinking beer—all of which leaves behind enough body cells to enable DNA profiling.[65] Not all of these traces are new. Fingerprints, for example, have long been available for government scrutiny. But many traces have only come into existence through the advent of ICT, while others can only be considered as traces because technological developments have enabled their identification as such. The increase in traces is enormous when we compare the digital and physical footprint of today's citizens with the footprint of citizens two decades ago, both in quantity and in quality.

Moreover, network technologies and digitization have enabled connecting these traces in many ways, effectively making citizens into digital persons[66] living their lives in databases.[67] The interconnection of traces can

---

INFORMATION COMMISSIONER BY THE SURVEILLANCE STUDIES NETWORK (David M. Wood ed., 2006), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf; Ben Bowling et al., *Crime Control Technologies: Towards an Analytical Framework and Research Agenda*, *in* REGULATING TECHNOLOGIES 51 (Roger Brownsword & Karen Yeung eds., 2008); JAMES C. FRASER & ROBIN WILLIAMS, HANDBOOK OF FORENSIC SCIENCE (2009); Bert-Jaap Koops, *Technology and the Crime Society: Rethinking Legal Protection*, 1 L. INNOVATION & TECH. 93 (2009).

65. Current DNA profiling requires only some dozens of picograms (i.e., 10^{-12} or a millionth of a millionth of a gram) of body material, the equivalent of four or five body cells, to make a DNA profile, provided the material is not contaminated. DNA profiles can therefore be made from material collected from single strands of hair, toothbrushes, cigarette butts, or smudges on a glass. *See* Peter Gill & Tim Clayton, *The current status of DNA profiling in the UK*, *in* HANDBOOK OF FORENSIC SCIENCE 29, 49 (Jim Fraser & Robin Williams eds., 2009).

66. *See generally* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (arguing that the existing privacy regulatory regime is uneven, overly complex, and ineffective at addressing the expansion in data compilation and retention on individuals).

67. *See generally* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN

also yield surprising results hitherto unimaginable, as illustrated by the development of DNA familial searching and digital profiling,[68] in which information about citizens is created using only data from other persons.

Within the power relations of law enforcement and citizens, the enormous increase in tracing capacity enabled by technology has been liberally embraced by the government in its role as law and order protector. Surfing the wave of the post-9/11 climate of fear,[69] as well as the more general and somewhat older wave of the risk society (i.e., a society that frames problems in terms of risks and that deals with hazards through systematic risk assessment and risk management),[70] the U.S. government has significantly broadened its surveillance powers over the past two decades. This has enabled the United States to surveil all citizens, in the dual sense of *sur-veiller* (i.e., "watching over"): care and control.[71] It has eagerly accepted the possibilities of the ever-increasing availability of personal data stored in existing databases, which are accessible to police and intelligence agencies through liberal data-ordering powers. It has also started to mandate the storage of personal data that would otherwise be deleted.[72] Furthermore, it has created extensive databases itself, such as DNA and PNR databases, which store data not about suspects of concrete crimes, but of varying collections of citizens who are, in varying degrees, seen as potential perpetrators of crime or terrorism. Technology is thus facilitating what is effectively a paradigm shift in the government's role in combating crime

---

THE 21ST CENTURY (2000) (discussing how advances in technologies endanger personal privacy).

68. *See generally* Mireille Hildebrandt, *Profiling and the Identity of the European Citizen*, *in* PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES 303 (Mireille Hildebrandt & Serge Gutwirth eds., 2008) (describing how the proliferation of automatically generated profiles in an increasingly networked society can affect the lives of ordinary citizens).

69. *Cf.* JONATHAN SIMON, GOVERNING THROUGH CRIME: HOW THE WAR ON CRIME TRANSFORMED AMERICAN DEMOCRACY AND CREATED A CULTURE OF FEAR (2007) (arguing that governing through crime fuels a culture of fear and control that in turn lowers the threshold of fear); CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE (2005) (discussing problems in individual and social judgments that can make people more fearful than is warranted).

70. *See generally* ULRICH BECK, RISK SOCIETY: TOWARDS A NEW MODERNITY (1992) (arguing that in a risk society, the "logic" of risk production outweighs the "logic" of wealth production).

71. DAVID LYON, SURVEILLANCE SOCIETY: MONITORING EVERYDAY LIFE 3 (2001).

72. Most notable is the mandatory retention of telecommunications traffic data in Europe. *See* Directive 2006/24/EC, 2006 O.J. (L 105) 54 (EU).

from an ex post, incidental, and last resort type of criminal law to an ex ante, comprehensive, and first resort type of criminal law.[73]

Now, how exactly does this affect the power relation of law enforcement and citizen? Law enforcement has acquired and is exercising considerably more power over ordinary citizens. The most poignant way the government can get a citizen to do what he would not otherwise do—by incarcerating him—has gained considerable momentum in the climate of "penal harshness" that has accompanied the risk society, particularly in the United States, but also in the United Kingdom and the Netherlands, a country that was once renowned for its mild and humane penal approach.[74] The expanded footprint of substantive law, constituted by the rise of regulatory crimes[75] and the criminalization of banal offenses or antisocial behavior,[76] implies that the punishing power of government is now exercised against wider circles of citizens.

However, what is more important for our analysis is that power is being exercised in new ways, beyond simply imprisoning or fining people. This is the architectural component of the surveillance society. Society's information processes are being structured in such a way as to enable continuous scrutiny of citizens for early warnings of abnormal and potentially dangerous behavior. As soon as the system gives off warning signals, restraint is exercised in ways more subtle than mere physical incapacitation, for example, by tracking rather than confining potentially dangerous subjects.[77]

---

73. Koops, *supra* note 64, at 117 (arguing that criminal law is shifting from a last resort to a primary tool of social control).

74. *See generally* DAVID GARLAND, THE CULTURE OF CONTROL: CRIME AND SOCIAL ORDER IN CONTEMPORARY SOCIETY (2001) (arguing that changes in criminal justice in the United States and the United Kingdom in the last twenty-five years are attributable to the social organization of modernity and the neoconservative politics that dominated in the 1980s); NICOLA LACEY, THE PRISONERS' DILEMMA: POLITICAL ECONOMY AND PUNISHMENT IN CONTEMPORARY DEMOCRACIES (2008) (discussing how British criminal justice policy has become increasingly politicized); Michael Tonry & Catrien Bijleveld, *Crime, Criminal Justice, and Criminology in the Netherlands*, *in* CRIME AND JUSTICE IN THE NETHERLANDS 1 (Michael Tonry & Catrien Bijleveld eds., 2007) (surveying the Dutch criminal justice system).

75. *See generally* Andrew Ashworth, *Is the Criminal Law a Lost Cause?*, 116 L. Q. REV. 225 (2000) (critically examining the expansion of criminal offenses to gain political favor); Robert Baldwin, *The New Punitive Regulation*, 67 MOD. L. REV. 351 (2004) (discussing evidence of a drift towards punitive approaches to regulation and more frequent imposition of criminal sanctions).

76. *See generally* Stuart Macdonald, *A Suicidal Woman, Roaming Pigs and a Noisy Trampolinist: Refining the ASBO's Definition of 'Anti-Social Behaviour,'* 69 MOD. L. REV. 183 (2006) (discussing the definition of antisocial behavior employed by the Crime and Disorder Act of 1998 for the purposes of the Anti-Social Behaviour Order).

77. *See* Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321 (2008) (arguing that legal

Foucault's recollection of Bentham's Panopticon as a paradigmatic way of disciplining people truly seems visionary: digital citizens in today's database nation cannot help but be aware of the watchful eye of the government's guards. It is not the fact of *being* watched, but the fact that at any moment they *can* be watched, that has a potentially disciplining effect on citizens. Perhaps it is this as much as any other factor that triggers the ubiquitous "I have nothing to hide" response[78]: a psychological mechanism of citizens to rationalize and therewith get to grips with the government's panoptic gaze. The implicit implication of "I have nothing to hide" is that "I don't mind being watched because I'm doing nothing wrong," and this precisely constitutes the normalizing, disciplining effect that Foucault's analysis of power elucidates. Through the panoptic power of surveillance architecture, citizens embrace society's prevalent paradigm of normality. This is not in itself good or bad, but it is an exercise of power in the relationship between government and citizen that must not be overlooked.

The increase in government power through the enlarged footprint of criminal law and the establishment of surveillance architectures is not offset by counter-developments that empower citizens. It is obvious that technology also opens up new paths for citizens, but these lie in the sphere of participatory democracy and electronic service delivery, and they do not generally affect the power relation of citizens with law enforcement. Technology does offer some options to citizens for shielding information, potentially more securely than is possible physically (e.g., with strong cryptography). However, on balance, technology facilitates the investigative ability of law enforcement and intelligence agencies much more than it enhances citizens' ability to evade authorities.[79] Simple privacy enhancing technologies (PETs) like drawing the curtains or whispering used to be quite effective against peeping Toms or eavesdroppers, but they are insufficient against modern home and body monitoring devices.[80] Furthermore, PETs for digital security are usually more complex and difficult to use than physical security devices. To be sure, some groups—organized and calculating criminals and terrorists—do benefit from technologies that allow them to

---

scrutiny of targeted forms of non-physical control has been overlooked).

78. *Cf.* Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007) (critically examining the argument that no privacy problem exists if a person has nothing to hide).

79. Koops, *supra* note 64, at 101.

80. *See generally* Bert-Jaap Koops & Merel M. Prinsen, *Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution*, 16 INFO. & COMM. TECH. L. 177, 180 (2007) (discussing how technological developments in ICT and DNA research pose a threat to home and bodily integrity).

hide from government scrutiny, and it is these groups that the new surveillance measures aim to combat. But compared to the traditional application of criminal law, the new measures are much less targeted and narrowly tailored. Thus, they are more likely to affect all citizens rather than small groups of suspects or would-be terrorists. In the arms race between governments and organized crime and terrorist groups, however legitimate and necessary it might be, ordinary citizens suffer massive collateral damage.

This collateral damage has two faces, each of which seems to require new forms of legal protection if a reasonable balance of power is to be maintained between government and citizens. First, citizens risk being wrongly involved in a government investigation. Some errors will always happen, because of human or technical imperfections, or due to the fact that profiling always involves some false positives, i.e., people who happen to fit a certain profile when in fact they do not belong to the category of people the profile aims at identifying. Errors may also occur because of criminal identity theft, which is a serious problem in both the United States and the Netherlands.[81] The risk of errors in crime fighting is not new, but the magnitude of the risk has grown with the rise of penal harshness and the expansion of surveillance databases. More importantly, it also involves other types of risk: the potential harm for citizens is not so much incarceration or even severe physical or emotional damage to home, body, or close relationships, rather it involves vague, invisible, and long-term forms of harm resulting from "data shadows" lingering in public and private databases. Perhaps the core vulnerability is no longer sending an innocent person to jail, but labeling the digital persona of an innocent citizen with a stamp that significantly lowers the quality of her future social life. Besides safeguards for proportional investigation and a fair

81. For the United States, see Michael W. Perl, *It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft*, 94 J. CRIM. L. & CRIMINOLOGY 169 (2003) (discussing the inadequacy of state identity theft laws to protect against criminal record identity theft in which an identity thief obtains a victim's personal information then commits crimes while acting as the victim). For the Netherlands, note the case of Mr. K, who was registered in government databases for over thirteen years as a serious drug criminal as the result of identity theft by a drug addict. Mr. K suffers significant obstacles in daily life; he is frequently held up at Schiphol Airport, receives numerous tickets for dodging transport fares, has had difficulty obtaining a mortgage, and has been subjected to a search in his home by thirty-five armed investigation officers, which induced him to move because all of his neighbors shunned him. The National Ombudsman castigated the government for their consistent failure to remove the man's registration data from its databases. *See* DUTCH NATIONAL OMBUDSMAN REPORT 2008/232 (2008), *available at* http://www.ombudsman.nl/nieuws/persberichten/2008/documents/Rapport20080232.pdf.

trial, new protection mechanisms should be introduced in the form of structural organized distrust within the neo-criminal justice system itself.[82]

The second face of the collateral damage to citizens is the disciplining effect of surveillance architectures. New forms of restraint, more subtle and varied than physical imprisonment, are imposed on groups encompassing more than just sophisticated criminals and terrorists. For example, ethnic minorities may be disproportionately stopped, frisked, and asked for identification in public spaces; antisocial people may be forced to comply with conditions of "Anti-Social Behaviour Orders";[83] and perpetrators of sexual offenses may be required to register for life in a sexual offender registry with community notification,[84] to name but a few affected groups.[85] Legal protection for these new forms of restraint is significantly underdeveloped.[86] This is eloquently illustrated by the U.S. Supreme Court's statement that "a statute that requires people to report for the rest of their lives to the government each time that they change hair color does not even invoke any constitutional scrutiny."[87] Moreover, citizens who are not directly restrained because they happen not to belong to a hapless category of "abnormal" people, are nevertheless affected by the government's panoptic power and may discipline themselves to conform to the prevalent paradigm of normality. Should this shift in the power relation between government and citizen not also be balanced by some new form of legal protection? This

82. Koops, *supra* note 64.

83. Anti-Social Behaviour Orders (ASBOs) allow authorities in the United Kingdom to impose an injunction on someone to refrain from further "antisocial" behavior, a breach of which is a criminal offense. *See* Crime and Disorder Act, 1998, c. 37 (Eng.); *see also* Macdonald, *supra* note 76 (arguing that ASBOs should be limited to repeat criminal offenders).

84. *Cf.* Jill S. Levenson & David A. D'Amora, *Social Policies Designed to Prevent Sexual Violence: The Emperor's New Clothes?*, 18 CRIM. JUST. POL'Y REV. 168 (2007) (arguing that sex offender registration and notification laws have not achieved their goals). Note that certain non-sexual offenders also end up in sexual offender registries. S*ee* Ofer Raban, *Be They Fish or Not Fish: The Fishy Registration of Nonsexual Offenders*, 16 WM. & MARY BILL RTS. J. 497, 499 (2007) ("[A] textbook example of negligent policymaking supported by faulty data and upheld by often poor judicial reasoning.").

85. *Cf.* DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 40 (2007) ("Controls are sought especially against 'undeserving' claimants and 'dangerous' offenders—and, even more, 'terrorists'—with the result that it is the poor and the marginal who are most deeply affected.").

86. *See* Murphy, *supra* note 77 (arguing that technologies of restraint are imposed without necessary procedural safeguards).

87. *Id.* at 191 (referring to an earlier discussion of *Connecticut Department of Public Safety v. Doe*, 538 U.S. 1 (2003), addressing Connecticut's "Megan's Law" that establishes a publicly available on-line sex-offender registry with photographs showing, among other things, the offender's hair color).

question will be revisited after first examining how other power relations are shifting.

IV. EMPLOYER–EMPLOYEE[88]

This Part examines technology-related changes in the power relation of employers and employees, and assesses the consequences of these changes for the legal protection of employees. While advances in ICT in recent years have lifted workplace constraints for many employees, these advances have also subjected workers to increased scrutiny. The following two case studies—workplace monitoring and location monitoring—suggest that the limits of employer surveillance will have to be renegotiated. It is questionable, however, whether current legal-protection mechanisms, which are largely based on transparency and consent, will suffice to empower employees to engage in renegotiation.

A. CASE STUDY 1: WORKPLACE MONITORING

The workplace has changed drastically with the introduction of ICT. Contrary to early fears—or hopes—that many workers would become redundant through the automation of office tasks, ICT has not led to the replacement of workers, but rather to significant changes in the nature and organization of work processes. The advent of the Internet, in particular, and the attendant introduction of e-mail as a standard tool for communication have changed the nature of the work floor. Cyberspace has emerged alongside physical space as the place where work is carried out and has led to a rise in telecommuting from home. Moreover, the walls of the workspace have become permeable: employees at the office are regularly in contact with the outside world without immediately visible or audible signs.

The introduction of ICT in the workplace has affected the power relation between employers and employees in different ways. At the empowering end of the spectrum, ICT has enabled employees to conduct activities they could not do before, or could only do to a limited extent, during working hours or from the office. For instance, employees can now make an appointment with the dentist, order groceries online, chat with a friend at the other side of the world, download pornography, or search the web for more interesting jobs.

88. *See generally* Colette Cuijpers, *ICT and Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning of Employees*, 25 J. MARSHALL J. COMPUTER & INFO. L. 37 (2007) (examining how ICT has affected the power balance between employer and employee and how adequately the existing legal framework has dealt with the resulting shifts in power).

The power of employers to make employees do what they would not otherwise do (e.g., work) has diminished somewhat as a result. More importantly, the power of employers to prevent employees from doing harm to the company has diminished. The huge number of outgoing SMS messages, e-mails, chats, and tweets, often drafted in informal language, could contain statements that are embarrassing or outright harmful for the company should they become public. Accounts of employees viewing or e-mailing pornography during work hours could also be damaging to a company's reputation. Finally, the risk that confidential business secrets or confidential documents may be leaked to third parties has grown substantially.[89] In these respects, ICT has weakened the power of employers.

In response, employers have taken countermeasures to rebalance the power relation. Primarily, they have started to routinely and extensively monitor employee communications. Workplace surveillance, by empowering the employer with new means of exercising control over employees, constitutes a shift in the power relation at the other end of the spectrum. A large majority of companies digitally monitor employee communications and activities.[90] Unsurprisingly, they often discover that employees are engaging in inappropriate activities and thereafter dismiss the employees.[91] Dismissal, of course, is one of the most far-reaching instruments of power employers possess (particularly during credit crunch crises), and the ability to dismiss

89. For an overview of liability risks for employers, see generally Michele Colucci, *The Impact of the Internet and New Technologies on the Workplace: A Legal Analysis from a Comparative Point of View*, *in* BULLETIN OF COMPARATIVE LABOUR (Roger Blanpain ed., 2002).

90. A 2007 survey by the American Management Association of 304 American companies showed that sixty-six percent monitor internet connections (and sixty-five percent block "inappropriate" websites); forty-five percent monitor computer activity, i.e., content, keystrokes, and time spent at the computer; forty-three percent monitor e-mail (over forty percent of which assign an individual to read e-mail); forty-five percent monitor telephones for time spent and numbers called, and sixteen percent record phone conversations; nine percent monitor voicemail; forty-eight percent use video surveillance to counter theft, violence, or sabotage, and seven percent use video surveillance to monitor on-the-job performance. Press Release, Am. Mgmt. Ass'n, 2007 Electronic Monitoring and Surveillance Survey: Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse (Feb. 28, 2008), *available at* http://press.amanet.org/ press-releases/177/2007-electronic-monitoring-surveillance-survey.

91. The Am. Mgmt. Ass'n survey showed that thirty percent of companies have fired employees for internet misuse, largely for viewing, downloading, or uploading inappropriate or offensive content (eighty-four percent), violation of any company policy (forty-eight percent), or excessive personal use (thirty-four percent); twenty-eight percent have fired employees for e-mail misuse, largely for violation of any company policy (sixty-four percent), inappropriate or offensive language (sixty-two percent), excessive personal use (twenty-six percent), or breach of confidentiality rules (twenty-two percent); and six percent have fired employees for misuse or private use of office phones. *Id.*

following workplace monitoring shows that technology is significantly empowering employers by strengthening the tools at their disposal.

In the United States, legal protection for the traditionally weaker party, employees, is found in privacy and employment law. However, the Fourth Amendment and the privacy tort of intrusion into seclusion have almost no bearing in light of the "reasonable expectation of privacy" doctrine. This is because the workplace is rarely considered a space where individuals may have any reasonable expectation of privacy, particularly when it comes to use of communication facilities provided by the employer.[92] ECPA protects communications privacy, but provides ample exceptions for employers, including the "provider exception," the "normal course of employment," and obtaining (implied) consent of the employee.[93] Employment law does not provide significant protection to employees against dismissal, because the doctrine of at-will employment still prevails.[94] Furthermore, exceptions to this doctrine developed in case law only apply in situations involving serious breaches of privacy.[95] Coupled with the absence of substantial privacy

92. *See* Cuijpers, *supra* note 88 (examining how ICT has affected the power balance between employer and employee and how adequately the existing legal framework has dealt with the resulting shifts in power); Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & PUB. POL'Y 609, 620, 619 (2009) ("[T]he employee's right of privacy is a hollow shell against the lead weight of the employer's claim to run his business as he pleases." (quoting Clyde W. Summers, *Individualism, Collectivism and Autonomy in American Labor Law*, 5 EMPLOYEE RTS. & EMP. POL'Y J. 453, 468 (2001))) ("Most people 'think they enjoy certain privacy protections when they are at work' but they do not."); Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829 (2005) (discussing the prevalence of employer monitoring of employees' e-mail and Internet use).

93. The "provider exception" allows any private employer who stores e-mail communications on her computer or network to access these communications. The "normal course of employment" exception applies when an employer can show that monitoring was necessary in the regular practice of employment, for example, to protect her company's property or to provide the internal communication service in a proper manner. The "consent" exception allows employers to monitor communications with the consent of employees, which includes implicit consent that may be affected when an employer gives prior notice to her employees that she will monitor e-mail communications. *Cf.* Cuijpers, *supra* note 88 (examining how ICT has affected the power balance between employer and employee and how adequately the existing legal framework has dealt with the resulting shifts in power); Rustad & Paulsson, *supra* note 92 (discussing the prevalence of employer monitoring of employees' e-mail and Internet use).

94. Katherine V.W. Stone, *Revisiting the At-Will Employment Doctrine: Imposed Terms, Implied Terms, and the Normative World of the Workplace*, 36 INDUS. L.J. 84, 85 (2007) ("[T]he contract is moment to moment for dismissal purposes but ongoing in relation to certain employer-imposed terms.").

95. Cuijpers, *supra* note 88 (examining how ICT has affected the power balance between employer and employee and how adequately the existing legal framework has dealt with the resulting shifts in power).

protection of employees, the current state of employment law offers no safeguard for employees against dismissal when workplace monitoring shows inappropriate conduct or breach of company policy.

On paper, employee protection in the Netherlands is more robust. European privacy law applies in the workplace context,[96] and European data protection legislation provides strict rules for processing personal data from employees.[97] Furthermore, frequent involvement of the Works Council in defining monitoring policies provide stronger checks on what a company can define as proper use of ICT. However, privacy law is seldom invoked in dismissal cases in practice;[98] courts usually take recourse in employment law under the general standards of "good employership" and "good employeeship."[99] Dismissal based on workplace monitoring takes into account three aspects: the grounds for workplace monitoring, the general principles of proportionality and subsidiarity, and the presence of a company policy with regard to Internet and e-mail use and monitoring. Even if the employer's monitoring was considered illegitimate or disproportionate, the dismissal is usually condoned by the courts if the employee's conduct did not conform to "good employeeship" or if the relationship between employer and employee has been seriously disrupted, which is usually the case.[100] Thus, even if employers abuse their power for workplace monitoring, employees who do not comply with company standards have little recourse to legal protection: they will not be reinstated in their job, nor will they get damages for breach of privacy.[101]

In summary, employees have gained new possibilities for communicating with the world outside the workplace and thus new opportunities for conducting personal activities during work hours. However, employer surveillance of employee communications has created a considerable risk of dismissal for employees if the employer decides that the activities observed are inappropriate, unlawful, or embarrassing to the company, or contrary to company policy. Legal protection, via privacy and employment law, provides employees with little recourse against dismissal if they have not conformed to what the employer has unilaterally defined as proper use of company

96. *See* Niemietz v. Germany, 16 Eur. Ct. H.R. 97 (1992); Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).

97. Directive 95/46/EC, *supra* note 58.

98. *Cf.* Frank Hendrickx, *Privacy and Data Protection in the Workplace: The Netherlands*, *in* REASONABLE EXPECTATIONS OF PRIVACY?: ELEVEN COUNTRY REPORTS ON CAMERA SURVEILLANCE AND WORKPLACE PRIVACY 115, 139 (Sjaak Nouwt et al. eds., 2005).

99. BURGERLIJK WETBOEK [BW] book 7, art. 611 (Neth.).

100. Cuijpers, *supra* note 88, at 55.

101. *Id.*

facilities. The Netherlands' legal protection appears to provide stronger checks on what a company can define as proper use than that of the United States, primarily due to the standard of good employership and the Works Council's hand in limiting monitoring policies.

B. CASE STUDY 2: LOCATION MONITORING

New ICTs not only enable monitoring of communications, but also facilitate monitoring individuals' locations. In recent years, the market for tracking and tracing devices has boomed and applications in the private sector have grown dramatically. However, employers' use of employee localization services is still limited when compared to communications monitoring.[102] The fact that location tracking may also take place outside of company premises and beyond working hours makes it a poignant new technology in the employer–employee relationship. Cuijpers distinguishes four technologies that can be used for location monitoring: video surveillance, radio frequency identification (RFID),[103] mobile phone cell ID, and the Global Positioning System (GPS) for use outside of company premises. For employers whose businesses involve transport, these technologies are particularly intriguing. This includes not only taxi or cargo companies, but also businesses with company vehicles or company mobile phones that can have an interest in monitoring their employees' whereabouts.

There are few specific laws regulating location monitoring of employees. The legal framework for location monitoring in the United States is much the same as that for communications monitoring.[104] There is little to no privacy protection of employees, despite the fact that GPS can provide detailed records of privacy-sensitive locations visited, such as doctors' offices, casinos, striptease clubs, or labor rallies.[105] Employers can easily nullify reasonable expectations of privacy by notifying employees of their location monitoring policy.[106] The fact that monitoring has become more intrusive due to location monitoring of vehicles, phones, and other company-provided gadgets, which easily extend outside of working hours and off premises, does

---

102. The AMA survey of 2007 showed that eight percent of companies use GPS for tracking company vehicles, three percent use GPS to monitor cell phones, and less than one percent use GPS for monitoring employee smartcards. Press Release, Am. Mgmt. Ass'n, *supra* note 90. However, fifty-two percent use smartcards to control physical security and access to buildings and data centers, which may also involve some form of location tracking. *Id.*

103. RFID uses radio waves for identifying and tracking objects or persons, which are particularly useful within company premises.

104. *See supra* Section IV.A.

105. *Cf.* State v. Jackson, 76 P.3d 217 (Wash. 2003).

106. Cuijpers, *supra* note 88, at 70–71.

little to alter the legal status of such monitoring. Absent specific legislative protection for employees,[107] companies can impose any policy governing use of the equipment they provide to employees.[108]

In the Netherlands, more specific rules apply for processing location data, as provided in the Telecommunications Act. These rules, however, apply only to publicly provided communications networks or services, and companies will often use private networks or services for intra-company monitoring. Moreover, the data protection rules for location services are an extremely complex amalgam, which makes it difficult for both providers and data subjects to interpret which rules apply to which data in which situations.[109] In the absence of workable specific rules for location data, the legal status of location monitoring in the Netherlands, like in the Unites States, is much the same as for communications monitoring.[110] This means that although protection for employees may be better on paper than in the United States, it remains to be seen whether this makes a material difference in practice.

C. DISCUSSION

The shifts in the relationship between employers and employees are more straightforward and less multifaceted than the shifts in the relationship between governments and citizens; the context in which this relationship takes shape, after all, is much smaller and simpler. The two case studies covered here—communication and location monitoring—address important aspects of employment, illustrating how intensively ICT has affected the nature of the workplace and the power relation between employer and employee. Two types of shifts take place in this power relation. On the one hand, employers lose power to control employees due to the ICT-facilitated permeability of the workplace, which allows employees to conduct more on-duty, non-work-related activities that pose higher risks for causing harm to the company. On the other hand, employers gain power to control employees by using comprehensive monitoring of communications and, increasingly, movement patterns, which may extend to off-duty and off-premises activities.

---

107. Statutory protection in federal and state law is limited and largely related to some specific activities, such as off-duty smoking. *See* Levinson, *supra* note 92, at 619.

108. *See* Press Release, Am. Mgmt. Ass'n, *supra* note 90 and accompanying text.

109. Collette Cuijpers & Bert-Jaap Koops, *How Fragmentation in European Law Undermines Consumer Protection: The Case of Location-Based Services*, 33 EUR. L. REV. 880 (2008).

110. Cuijpers, *supra* note 88 at 73.

The shifts in the power relation are symmetrical in that the increased surveillance of the workspace is a direct result of the increased permeability of the workspace. To the extent that employees benefit from new opportunities offered by ICT in the employment context, they are also under increased scrutiny when they use these new opportunities. Although this might imply that the shifts counterbalance each other, some aspects must be taken into account before we can draw conclusions about the legal protection of the traditionally weak party in this context.

First, the shifts in the power relation, even if they are symmetrical, broaden the context of employment considerably. The permeability of the workspace comes along with a blurring, both in spatial and in temporal terms, of work and private life. The exercise of power by the employer therefore gains a wider scope of application. Perhaps unlawful or inappropriate behavior by employees, even off-duty, has always been sufficient cause for dismissal, but the chances of observing such behavior and collecting demonstrable evidence of it are considerably higher as monitoring of employee behavior widens.

Second, notification duties play a crucial role. Since most of the ICT monitoring is invisible, employees may not be aware of the monitoring unless the employer has told them in advance. Because serious potential consequences—notably dismissal—can follow depending on what the monitoring uncovers, it is justified to at least notify employees of the monitoring system and the associated policy. Yet in the United States, only a handful of states have legislation requiring notification of electronic monitoring.[111] In contrast, in the Netherlands, notification is one of the core principles of data protection legislation[112] and a guideline in the Dutch Data Protection Authority's Framework Policy for E-Mail and Internet Use.[113] A further mechanism for alerting employees about employee monitoring is included in the Dutch Works Councils Act, which requires that personnel tracking systems [*personeelsvolgsystemen*] are approved by the Works Council.[114] Admittedly, having a notification duty on paper does not necessarily guarantee that employees are actually made aware; that will depend on the

111. Phillips, *supra* note 49; Levinson, *supra* note 92, at 622 (referring to CONN. GEN. STAT. § 31–48(d) (2009); DEL. CODE ANN. tit. 19, § 705 (2002)).

112. *See* Wet bescherming persoonsgegevens [Personal Data Protection Act], Staatsblad van het Koninkrijk der Nederlanden [Stb.] 302 (2000), ch. 5 (Neth.).

113. *See* College Bescherming Persoonsgegevens, *Raamregeling Voor Het Gebruik van E-mail en Internet* (2002), *available at* http://www.cbpweb.nl/downloads_av_sv/AV21_raamregeling.pdf?refer=true&theme=purple.

114. *See* Dutch Works Councils Act art. 27(1)(1).

implementation in practice, for example, in what form and when the notification takes place.[115]

A third relevant aspect is whether the company policy governing the use of company facilities, including computers, Internet, mobile phones, and vehicles, strikes a fair balance between employer and employee interests. Again, there seem to be better legal safeguards in place in the Netherlands. For instance, the Works Councils Act requires works councils to approve monitoring policies and a provision in the criminal law prohibits "obvious misuse" by the employer of his right to monitor employee communications.[116] In the United States, collective bargaining mechanisms and the National Labor Relations Act may provide some safeguards, but these are limited in scope and scale.[117] Levinson has argued that the "law of the shop" as applied by arbitrators should be used more widely to provide better safeguards to employees against arbitrary monitoring.[118]

Together, these aspects caution against concluding that the empowering and disempowering shifts in the employer–employee relationship counterbalance one another. The broadening of the scope of employer monitoring, both within the workplace and off-duty and off-premises, is not necessarily balanced by the mechanisms for curbing the employer's power, if notification and supervision of the fairness of monitoring policies are largely absent, which seems the case in the United States but also, perhaps, in the Netherlands due to the lack of enforcement of privacy protection in dismissal cases.[119] Moreover, even if the policy is fairly balanced and employees are duly notified of it, the stakes are higher for employees nonetheless: employees are under more prevalent scrutiny, and at times and in places that used to be reserved for purely private, non-work-related activities.

---

115. For example, in small print in a leaflet about company policies given to new employees on their first day of work or hidden somewhere in an attic room of the company's internal homepage—neither of which is very likely to truly inform employees—or, at the other extreme, by a notice appearing on the screen each time the employees log in on their computer.

116. DUTCH CRIMINAL CODE art. 139c(2)(2).

117. Levinson, *supra* note 92 at 622; *cf.* M.W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 498 (2002) (noting that "the percentage of the civilian labor force eligible for union representation that actually is unionized, has fallen to a post-War low of 9.4%").

118. Levinson, *supra* note 92, at 639; *see also* National Academy of Arbitrators, http://www.naarb.org/ (last visited Sept. 25 2009).

119. *See supra* note 88 and accompanying text.

This parallels the two types of collateral damage to citizens caused by the arms race in criminal investigation: the risk of interpretation errors and the mass disciplining and normalization of behavior by employees.[120]

Increased monitoring of employee behavior has amplified the risk of errors. For example, if a civil servant searching for public policy information absent-mindedly types in www.whitehouse.com (instead of .gov) or www.amsterdam.com (instead of .nl) and finds himself confronted with flashy X-rated pictures,[121] can the monitoring system distinguish him from an employee who is actually surfing for adult material? If an employee has to deliver a package in the center of Amsterdam and, due to road renovations and subway constructions, gets lost and ends up in the red-light district, does he have a defense against the proof of the car tracking system? Or what if his nineteen-year-old son "borrowed" the car for an excursion into red-light nightlife? Such errors in interpretation, including technical errors, can and will usually be redressed somewhere in the procedure. Sometimes, however, it might be too late; the procedure itself may have a negative effect on the employer–employee relationship.[122] For example, an employer's false accusation may have induced the employee to circulate enraged messages among his colleagues with insulting remarks about his employer.

More important is the mechanism, comparable to the increased footprint of criminal law to cover trivial offenses or antisocial types of behavior, of sanctioning employees for undesirable off-duty or off-premises activities that do not cause significant harm to the employer, but that nonetheless fall within the ambit of "unacceptable" behavior as defined by the employer. Although off-duty and off-premises monitoring does not yet take place on a large scale, when it happens it has significant potential effects on the freedom of employees to behave as they wish.

Here, we encounter the second face of collateral damage to citizens: the potentially disciplining effects of ubiquitous surveillance. Although stricter limits apply to the monitoring powers of employers when it comes to off-duty behavior, monitoring is allowed to a degree by employment or privacy

120. *Supra* Section III.D.

121. Both sites nowadays are relatively respectable-looking websites, but they started out as porn websites. *See, e.g.*, Lodewijk F. Asscher, *Schuldige domeinnamen*, 10 COMPUTERRECHT 186 (2003); Jeff Pelline, *Whitehouse.com Goes to Porn*, CNET NEWS, Sept. 5, 1997, http://news.cnet.com/2100-1023-202985.html.

122. *See generally* Cuijpers, *supra* note 88 (referring to J. Yung, *Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should do About It*, 36 SETON HALL L. REV. 163, 180 (2005), noting the risk of abuse of power: employers could use a relatively harmless incident to fire an employee if they want to get rid of her for other reasons that might be less successfully argued in court).

law, particularly if it concerns employer-provided equipment, such as a cell phone or computer.[123] Awareness that the employer is potentially monitoring activities conducted with such equipment could lead to (over)cautiousness in the use of the equipment. Although an employee could refrain outright from using company equipment for personal purposes, that option does not alight with the reality of the "new economy." Private use of employer property

> is often regarded as a kind of fringe benefit. Employees expect some leniency with regard to the private use of company assets, and the employer often encourages this use to circumvent employees' nine-to-five mentality. A lot of companies provide employees with home computers or mobile telephones which they can use for private purposes. The added value for employers lies in the fact that the employee can be reached for business related purposes 24-hours-a-day.[124]

In this new constellation of blurred boundaries between office and home, and working hours and spare time, the limits of employer surveillance will have to be renegotiated. It is not clear, however, that current legal mechanisms for employee protection provide employees with sufficient bargaining power in this renegotiation process. The easy way out may well be to accept the increased monitoring scope and to normalize private behavior in a self-disciplining act of conforming to the company standards for acceptable behavior.

Internalizing acceptability standards contributes to the erosive effect of technology on privacy.[125] David Phillips calls attention to the "vicious circularity" of ever more invasive surveillance techniques at the workplace:

> courts have found that employees reduce or extinguish their reasonable expectation of privacy when they explicitly consent to employers' search policies. Employers, then, demand such consent as a matter of standard business practice. That standard practice then becomes implicit in the community norms generally governing the workplace surveillance. Eventually, consent to search becomes implicit in the employment relationship.[126]

---

123. Levinson, *supra* note 92.

124. Cuijpers, *supra* note 88, at 85.

125. *See generally* Bert-Jaap Koops & Ronald Leenes, *"Code" and the Slow Erosion of Privacy*, 12 MICH. TELECOMM. & TECH. L. REV. 115 (2005) (finding that technology generally makes privacy violations easier and erodes reasonable expectations of privacy).

126. Phillips, *supra* note 49, at 60.

Communications monitoring can already be called a standard practice; location monitoring is only beginning to be included in employer policies.[127] If both types of monitoring continue in the vicious circularity of ingrained, normalized standards, then the workplace will acquire distinct characteristics of the Panopticon and Foucauldian self-disciplining effects on employees. Current protection mechanisms based on transparency (notification) and consent (employment at will) seem inadequate to deal with such a shift in the power relationship between employers and employees.

V. BUSINESS–CONSUMER[128]

This Part examines technology-related changes in the power relation of businesses and consumers, and assesses the consequences of these changes for consumer protection. The two following case studies—profiling and behavioral advertising and buying goods or services online—suggest that, although both consumers and businesses gain substantially in their information position, businesses gain considerably more power to seduce consumers to buy goods that they would not otherwise buy. The subsequent general discussion will analyze whether current legal measures of consumer protection are equipped to deal with businesses' exercise of power. Particularly relevant here is the second dimension of power: the indirect influencing of consumers' actions through "agenda-setting" mechanisms of targeted advertising and website design.[129]

A. CASE STUDY 1: PROFILING AND BEHAVIORAL ADVERTISING

Commerce often starts with advertising. Traditionally, this is a fairly crude mechanism. Advertisements are directed at a large group of people who happen to read the same newspaper or watch the same television channel; and businesses can only target their advertising to the extent that they know something about the average consumer of the medium. ICT is enabling the use of profiling techniques to offer personalized advertising to consumers. This mechanism is relatively new and qualitatively different from the traditional information position of businesses. Profiling provides a new type of knowledge, based on patterns discovered by correlating data in

127. *See generally* Cuijpers, *supra* note 88.

128. This Section builds on Colette Cuijpers, *The Influence of ICT on Consumer Protection: Empowerment or Impairment of the Consumer?* (TILT Law & Tech. Working Paper Series, Paper No. 015/2009, 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1515790.

129. See *supra* note 6 and accompanying text for a discussion of the second dimension of power.

databases.[130] Information about consumption patterns, such as different products that certain types of consumers often buy together or types of books that people with certain characteristics are more likely to buy, can be used to target advertising to specific consumers in concrete contexts. Rather than displaying any advertising banner, a website may choose a specific advertisement based on the prospective buyer's clickstream, search words, zip code, or other data that the user has filled in on a web form.

Such personalized or behavioral advertising is a promising innovation in commerce. Since it customizes the advertising to align with the consumer's inferred interests, it can be more effective for both businesses and consumers. Indeed, personalization can be "an effective tool to achieve an efficient market."[131] However, the promise does not come without threats. Behavioral advertising is usually based on group profiles, which will almost always be probabilistic and non-distributive, i.e., not all members of the group defined by the profile will share all the attributes of the group profile.[132] In other words, false positives are bound to occur: someone who has bought Koontz's *Mr. Murder* and Weldon's *The Cloning of Joanna May* because she is interested in fiction about clones may not be at all interested in other pulp thrillers or feminist novels. Some targeted advertisements will therefore miss their mark, through false positives and false negatives. Although this may lead to "unanticipated encounters" in which consumers are confronted with undesirable or irritating information that they have not sought out,[133] this is not generally a serious threat. Compared to traditional, non-personalized advertising, the error rate, particularly of false positives, will be much lower and missed opportunities for advertising do not impair the ability of consumers to buy goods of their own initiative.[134]

---

130. Mireille Hildebrandt, *Defining Profiling: A New Type of Knowledge?*, *in* PROFILING THE EUROPEAN CITIZENS 17 (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

131. Simone van der Hof & Corien Prins, *Personalisation and Its Influence on Identities, Behaviour and Social Values*, *in* PROFILING THE EUROPEAN CITIZEN 111 (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

132. *See* BART HERMAN MARIA CUSTERS, THE POWER OF KNOWLEDGE: ETHICAL, LEGAL, AND TECHNOLOGICAL ASPECTS OF DATA MINING AND GROUP PROFILING IN EPIDEMIOLOGY 61 (2004) (discussing non-distributivity).

133. Cass R. Sunstein, *The Daily We: Is the Internet Really a Blessing for Democracy?*, BOSTON REV., Summer 2001, *available at* http://bostonreview.net/BR26.3/sunstein.html.

134. There may be a concern, however, if the targeted advertising is based on sensitive data, even if the consumer is not personally identifiable; consumers can then "view it as invasive or, in a household where multiple users access one computer, it may reveal confidential information about an individual to other members." Press Release, Fed. Trade Comm'n, Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles 5 (Dec. 20, 2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf. *But cf.* van der Hof & Prins, *supra* note 131.

There is a more subtle and serious threat being exercised in behavioral advertising, which relates to the second dimension of power.[135] By personalizing the offers shown to online consumers, businesses influence the horizon of consumers' interest: it is a form of agenda-setting. This "may force individuals into restrictive two-dimensional models,"[136] reducing the consumer's areas of interest into simplified machine-readable patterns and resulting in a potential loss of nuances and of occasional side-steps into marginal or new areas of interest. It may also lead to normalization of consuming behavior, through the panoptic logic of "the system":

> [w]hen the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? . . . [P]rofiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the patterns; the cycle begins again.[137]

In other words, if you are persistently being offered pulp thrillers and feminist novels because your online bookshops think you should be interested in them, you might as well give it a try because there should be some merit to the recommendations (why else would the system give them?), thereby reinforcing your profile and leading to more of the same offers. Thus, you might well end up reading only these types of books because it is—by the system and through panoptic logic by yourself—expected of you.

How do current legal-protection mechanisms deal with behavioral advertising? In general, data protection cannot be invoked as long as group profiles are being used to show ads to unidentifiable online consumers.[138] However, if a European consumer is identifiable, for example by an IP address,[139] when showing her an ad based on a group profile of certain online

---

135. See *supra* note 6 and accompanying text for a discussion of the second dimension of power.

136. Van der Hof & Prins, *supra* note 131, at 121.

137. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 154 (1999).

138. This constitutes one of the weaknesses of the Data Protection Directive in an online environment, since potential privacy or discrimination threats to web users often do not depend on their being identifiable as Jill the Plumber from Tuscaloosa, Alabama, but on their being recognized as being the same person as an earlier website visitor or their being traced throughout a session. *See* Ronald E. Leenes, *Do You Know Me? Decomposing Identifiability* (Tilburg Univ. Legal Studies, Working Paper No. 001/2008, 2008) (distinguishing between L-identifiability ('looking-up'), R-identifiability ('recognition'), and S-identifiability ('session')).

139. IP addresses can be considered as personal data. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 4/2007 ON THE CONCEPT OF PERSONAL DATA

behavior or personal characteristics, her personal data are covered within the ambit of the Data Protection Directive. The Directive also applies to the collection of behavioral or personal information from identifiable consumers. This theoretically could provide some legal protection, for example, against disproportionate collection of data or application of a "wrong" group profile; but it is highly dubious whether the Directive can actually be enforced in such a context.[140]

In the United States, no specific data protection rule seems to apply to the collection of data and the display of advertisements in this context. The Federal Trade Commission (FTC), however, has recommended that

> [e]very website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose.[141]

Much of the efficacy of such a recommendation will depend on how consumers are being informed and given a choice—only a handful of knowledgeable and privacy-aware consumers might be able to understand and act upon the issue.[142] Moreover, it remains to be seen whether business self-regulation as advocated by the FTC really works in this area.

16–17 (2007), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf. This is not uncontested in the literature, but Opinions of the Article 29 Data Protection Working Party serve as important guidelines for courts in the E.U. to interpret the Data Protection Directive.

140. One wonders what Amazon.co.uk would include in a reply to a request from a Dutch customer such as:

> Could you inform me on what basis you recommended E.M. Forster's *Maurice* and Baldwin's *Giovanni's Room* to me (*see* Wet bescherming persoonsgegevens [Dutch Data Protection Act], art. 35), whether this relates to my having bought Leavitt's *The Lost Language of Cranes* last month (*see id.* at art. 33) and whether you have therefore profiled me as being interested in homosexuality, which is sensitive personal data (*see id.* at art. 16), and would you please delete all these data since it is unlawful for you to process them (*see id.*) and irrelevant for my buying books with you (*see id.* at art. 36(1)), and can you inform me in writing of your having deleted my sensitive personal data (*see id.* at art. 36(2))?

141. Press Release, Fed. Trade Comm'n, *supra* note 134, at 3.

142. *Id.* (noting that "panelists recognized that many consumers do not read privacy policies and raised a genuine question about consumers' willingness and ability to read and understand long disclosures about privacy").

Specifically relevant in this case study is the legal protection against deceptive advertising. This, after all, is the true concern about enticing consumers to buy goods they would not otherwise buy. Deceptive advertising is thus seen as an abusive exercise of power by businesses; to protect consumers, this is prohibited both in European and U.S. legislation.[143] However, as with data protection rules, this legal protection will be difficult to enforce; consumers are often unaware of the practice, and even if they are, the damage for each individual consumer deceived by a behavioral advertisement will usually be relatively low compared to the time, money, and tools they have to invest in pursuing a contract or tort claim.[144] More importantly, however, it is not clear whether behavioral advertising is at all deceptive. The purpose, after all, is to better target the offer to the consumer's own preferences, and the personalization as such does not make it manipulative. Only the agenda-setting and interest-shaping aspect of behavioral advertising could be considered deceptive for consumers who embrace the profile underlying the advertisement through panoptic logic,[145] even though they had no obvious prior interest in the offered product. But it is unlikely that this subtly manipulative effect, which works through an act of double anticipation by the consumer herself,[146] is sufficient to fall within the scope of deceptive advertising rules.

B. CASE STUDY 2: BUYING ONLINE

The advent of e-commerce has provided consumers not only with a new means to do old business—buying goods or services—but also opened up a far wider range for conducting this business. Rather than leaving their homes to shop locally, consumers can now search for goods around the world. With automated search engines, websites comparing products and prices, and

143. *See, e.g.*, Directive 2005/29/EC, 2005 O.J. (L 149) 22 (EC); Federal Trade Commission Act, 15 U.S.C. §§ 42–58 (2006); Lanham Act, 15 U.S.C. § 1125(a) (2006).

144. *See* Marla Pleyte, *Online Undercover Marketing: A Reminder of the FTC's Unique Position to Combat Deceptive Practices*, 6 U.C. DAVIS BUS. L.J. 14 (2006); Willem van Boom & Marco Loos, *Effective Enforcement of Consumer Law in Europe: Private, Public, and Collective Mechanisms*, *in* COLLECTIVE ENFORCEMENT OF CONSUMER LAW 231 (Willem H. Van Boom & Marco Loos eds., 2007).

145. *See supra* note 137 and accompanying text.

146. I.e., the consumer changes her preferences—buying a product she would not otherwise have bought—in anticipation of the interest profile she thinks is reflected in the advertisement that anticipates her preferences. On the similar mechanism of double anticipation in identity building, see WP7, D7.14A: WHERE *IDEM*-IDENTITY MEETS *IPSE*-IDENTITY: CONCEPTUAL EXPLORATIONS (Mireille Hildebrandt et al. eds., 2008), *available at* http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP7-del7.14a-idem_meets_ipse_conceptual_explorations.pdf. *See also infra* Section VI.A.

auction and trading sites, consumers have an array of tools available to help them find the best products for the lowest prices.

There are more aspects in which ICT is empowering consumers. They can form ad hoc online collectives that use mass buying to obtain the lowest possible price from e-sellers.[147] Similarly, businesses are being profiled by ad hoc collections of consumers who together build and maintain ratings websites with assessments of businesses' quality, service level, and reliability. A hotel owner now must not only be friendly to Mr. Michelin or Miss Lonely Planet when they visit once a year, but to each and every customer, or risk receiving unfavorable reviews on a rating website.

This does not imply, however, that the Internet constitutes a Shangri-La of pervasive consumer power. Rating and experience-sharing websites are not necessarily reliable:

> [t]his valuable source of information is diminished when online undercover marketers are allowed to surreptitiously infiltrate such sites and plant self-interested messages about their products. These advertisers are well-funded and sophisticated enough to craft messages that are extremely believable and likely to induce consumer reliance. As a result, these practices turn a valuable source of information into a source of disinformation for consumers.[148]

In other words, the potentially most powerful tool for consumer empowerment—peer review—may backfire, since businesses can turn it to their own advantage to seduce consumers to buy their products.

When we focus on the actual online buying process, we observe that consumers no longer depend on the local bookstore or camera shop; they also can shop from their desk chair for the best deal in as large a region as they care to explore. Moreover, websites allow for a full presentation of the general terms and conditions, rather than a scant reference to paper documents that can be inspected somewhere or snail-mailed upon request. E-consumers thus have, in principle, a much wider scope for buying as well as better knowledge of the product and the terms and conditions covering the sale.

---

147. Robert J. Kauffman & Bin Wang, *Bid Together, Buy Together: On the Efficacy of Group-Buying Business Models in Internet-Based Selling*, *in* THE E-BUSINESS HANDBOOK 99 (Paul Benjamin Lowry et al. eds., 2002). For examples of collective buying sites, see, for example, Groupon Deal of the Day: Find Great Deals on Fun Things to Do in San Francisco, http://www.groupon.com/ (last visited Sept. 25, 2009) and Pingel Partner, http://www.pingelpartner.nl/ (last visited Sept. 25, 2009).

148. Pleyte, *supra* note 144.

Several obstacles, however, decrease the empowering potential of online buying. A website's design can make a business' terms and conditions difficult to find. Alternately, consumers are increasingly presented with terms and conditions before they can make a purchase. However, because the terms and conditions are obfuscated by legalese and small print, few e-consumers will read and understand these terms. Furthermore, a physical product cannot be seen, let alone touched and immediately taken away. Thus, the consumer has to rely on pictures and on the seller's reliability to send the correct product depicted in the image.

This uncertainty is offset by increased options for redress. The European Distance-Selling Directive, for example, allows consumers to return online-purchased goods without providing a reason within seven days.[149] Still, returning a defective good will not always be cost-effective for consumers if the defect is relatively small—receiving a yellow coffee machine when you thought you were ordering an orange one—particularly if the consumer needs to spend precious time on repackaging and going to the post office. Finally, "scattered damage" (i.e., many trifling losses that are too minor for individuals to seek redress for, but that constitute a significant loss on a collective scale) is a problem that will occur more frequently as e-commerce expands.

Perhaps the biggest obstacle is that these downsides are exacerbated in the cross-border context of online commerce. Terms and conditions are not necessarily available in one's own language (particularly for native speakers of relatively small languages, such as Dutch, Italian, or Hungarian, not to mention minority languages like Frisian or Kwakiutl). The contract may be embedded in foreign legal systems with possibly unfamiliar rules and presuppositions. And redress is more costly and cumbersome when returning a package to businesses abroad. Some mechanisms for cross-border redress are starting to emerge, for example, in the network of European Consumer Centres.[150]

Another relevant aspect is what happens with the consumer data that are gathered by businesses throughout the process. ICT can empower businesses, who can gather huge amounts of information about consumers through mechanisms such as cookies and web forms. Privacy statements will inform consumers about the purposes and conditions for processing the personal data collected during e-commerce activities, but it is unclear how

149. Directive 97/7/EC, art. 6, 1997 O.J. (L 144) 19 (EC).

150. *See* ECC-Net, http://ec.europa.eu/consumers/redress_cons/index_en.htm (last visited Feb. 4, 2010).

many consumers actually find, read, and understand privacy statements. Even if they do, it is not clear to what extent they can effectively resist undesirable provisions—such as selling data to third parties—in a market that is dominated by information brokers.

The legal protection of consumers has already been adapted in several respects to the new reality of e-commerce, at least in Europe. The E.U. "Consumer Acquis" consists of many directives with consumer-protection rules.[151] Particularly relevant here are the Unfair Commercial Practices Directive and the Distance Selling Directive.[152] These contain numerous information obligations, such as requirements to provide information beforehand in a comprehensible and durable form,[153] and balancing requirements to enhance the fairness of terms and conditions.[154] The current framework of European consumer protection, nevertheless, is very fragmented, and a new Directive on Consumer Rights has been proposed that aims to bring together and harmonize key consumer rights.[155] In contrast to the European legislative approach, "[t]he U.S. legal system has tried, at times awkwardly, to fit the new transactions into existing doctrinal categories,"[156] which leaves consumer protection primarily to the market.

Altogether, the information gains that the Internet allows constitute a significant shift towards consumer empowerment. However, this empowerment is lessened by several factors, such as the risk of information overload and the non-transparent nature of many information providing websites that may manipulate results for commercial reasons. Nevertheless the information position of ICT-savvy consumers is superior to their information position in traditional, physical-space commerce. The scope for buying goods has also expanded enormously, and despite obstacles for e-commerce, notably in cross-border contexts, this can likewise be seen as a

151. The "Consumer Acquis" is an umbrella term used to indicate the widespread collection of consumer-protection rules in E.U. legislation. *See generally Proposal for a Directive of the European Parliament and of the Council on Consumer Rights*, COM (2008) 614 final (Oct. 8, 2008) (reviewing the Consumer Acquis, including a number of directives on consumer protection, and proposing changes to simplify and harmonize the current fragmented regulatory framework).

152. Directive 2005/29/EC, *supra* note 143; Directive 97/7/EC, *supra* note 149.

153. *See* Directive 97/7/EC, *supra* note 149, at art. 4–5; Directive 2000/31, art. 5, 6, 10, 2000 O.J. (L 178) 1 (EC).

154. *See* Directive 2005/29/EC, *supra* note 143, at art. 3.

155. *Proposal for a Directive of the European Parliament and of the Council on Consumer Rights*, COM (2008) 614 final (Oct. 8, 2008).

156. Jane K. Winn & Brian H. Bix, *Diverging Perspectives on Electronic Contracting in the U.S. and the EU*, 54 CLEV. ST. L. REV. 175, 190 (2006).

significant empowerment of consumers, supported as they are by new consumer-protection rules in legislation or case-law doctrine.

Some caution is warranted, however, when it comes to assessing the overall effect on consumers at large: not all consumers benefit equally from the new possibilities. These new possibilities are perhaps real options only for experienced ICT users with a sufficiently perceptive and critical attitude to web-based information sources. Furthermore, the information position of businesses is also strengthened considerably, through information- collecting, sharing, and profiling tools. They can use this information to better attract and bind consumers to them. Just as consumers have access to a broader array of businesses, businesses also have significantly increased their capability for finding customers. With the varied effect on different types of consumer groups, this implies that less ICT-savvy and less critical consumers may now be more vulnerable to abusive exercises of power by businesses.

C. DISCUSSION

The commerce context presents perhaps the most empowering potential of ICT yet encountered in the case studies. The Internet has opened up a wide range of opportunities for consumers to counter businesses' efforts to seduce them into buying their products and services. Gathering information, shopping irrespective of place, and forming consumer collectives are important consumer-empowering mechanisms. One might question to what extent all consumers benefit from these possibilities: perhaps only the technology-savvy consumers are exploiting them in practice. Compared to the other power relations studied here, consumers benefit more from new technology-facilitated opportunities than citizens in their relationship with the government, but perhaps less than employees in their relationship with the employer. Determining to what extent the "average" consumer actually makes use of information-gathering and collective-pressure mechanisms is a matter for further study.[157]

157. The current legal status of the average consumer with respect to her ICT awareness or tech-savviness is indeterminate. For example, European Court of Justice case-law on the free movement of goods and services seems to assume a relatively high level of activity and knowledge of consumers, whereas the Consumer Acquis—the fragmented system of consumer protection in many first-pillar Directives—seems to treat the consumer as relatively passive and poor-informed. *See* Hannes Unberath & Angus Johnston, *The Double-Headed Approach of the ECJ Concerning Consumer Protection*, 44 COMMON MKT. L. REV. 1237 (2007); Vanessa Mak, *Harmonisation Through 'Directive-Related' and 'Cross-Directive' Interpretation: The Role of the ECJ in the Development of European Consumer Law* (Tilburg Inst. of Comparative & Transnational Law, Working Paper No. 2008/8, 2008).

At the same time, ICT also has significant empowering effects for businesses, who can gather huge amounts of information about consumers, both specifically through tools like cookies and web forms and generically through profiling. They can also target consumers cost-effectively with advertisements and offers, on a massive scale unimaginable in the pre-ICT era (i.e., spam) but also on an individual, personalized level (i.e., behavioral advertising).

Both consumers and businesses have thus gained substantially in their information position. Like the case of employers and employees, it is far from evident that these trends counterbalance each other, particularly since the trends are less clearly intertwined than in the workplace monitoring cases.[158] With some justification, Dholakia and Zwick conclude that "[t]he power balance has shifted to the marketers."[159] After all, the strengthened position of businesses gives them considerable power to seduce consumers to buy goods they would not otherwise buy.

This increased power can only be outweighed by the empowering information-gathering possibilities for consumers, provided that the business activities are sufficiently transparent for the consumer. This is a key issue both in behavioral advertising and in online buying with impenetrable terms and conditions and privacy statements. Does the consumer in these situations know on what basis she is being offered something, or what will happen with the personal data that are collected when she buys something online? The legal protection of consumers has been adapted in some respects to the new reality of e-commerce, through information obligations aimed at enhanced transparency.[160] Such measures surely help to balance the power relation, but they are probably insufficient to protect consumers in all

158. *See supra* Section IV.C.

159. Nikhilesh Dholakia & Detlev Zwick, *Privacy and Consumer Agency in the Information Age: Between Prying Profilers and Preening Webcams*, 1 J. RES. FOR CONSUMERS 18–19 (2001), *available at* http://www.jrconsumers.com/academic_articles/issue_1?f=5800. As they observe,

> real-time customization of interactive messages can actually limit the ability of the consumer to shape his or her ideas of market prices, product variability, and quality, among other things. In such a scenario—of which we can see the first signs in the electronic marketspace—real-time interactivity does not enable consumer choice and informed decision-making, but delimits consumer freedom and unrestrained agency in the market.

Id. at 12–13; *cf.* LYON, *supra* note 71, at 127–28 (noting that "while the public awareness of consumer surveillance may be rising, it is undoubtedly doing so at a rate far slower than the opportunities for consumer surveillance are being exploited").

160. *See supra* note 151 and accompanying text.

respects. Several authors stress that more legal protection is needed to decrease the information asymmetry between consumers and business,[161] to increase transparency,[162] and to allow more room for collective action in order to address the problem of large amounts of small individual damages where access to justice for individual consumers is unattractive.[163]

Two issues also call for attention, relating closely to the two faces of collateral damage identified in the government–citizen power relation shifts.[164] First, the consumer has become more vulnerable through the increased collection and storage of personal data. Not only can these data be used for other purposes—for example, when sold to third parties—but they can also be leaked through inadequate security measures, and subsequently be used for financial identity theft.[165] The lack of a potent and practically enforceable data protection regime[166] is apparent. Also, the occurrence of interpretation errors may be relevant; for example, the product searched for or bought might be for someone else—a gift, a purchase for a bed-ridden neighbor, or a family member to whom you lent your credit card. This will not always lead to concrete damage, but the erroneous profile thus

---

161. *E.g.*, Hildebrandt, *supra* note 68, at 308; Els Soenens, *Web Usage Mining for Web Personalisation in Customer Relation Management*, *in* PROFILING THE EUROPEAN CITIZEN: CROSS-DISCIPLINARY PERSPECTIVES 175, 180 (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

162. Detlev Zwick & Nikhilesh Dholakia, *Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing*, 24 J. MACROMARKETING 31, 40–41 (2004) (arguing that "the power to constitute consumer identity . . . is located within the database and that 'only if consumers are given full access to companies' customer databases can they maintain a sense of control over their identities in the marketplace").

163. Van Boom & Loos, *supra* note 144.

164. *See supra* Section III.D; *see also supra* Section IV.C.

165. *See, e.g.*, Jennifer A. Chandler, *Negligence Liability for Breaches of Data Security*, 23 BANKING & FIN. L. REV. 223 (2008) (discussing the need for civil liability to increase data security and problems plaintiffs face in civil lawsuits); Sasha Romanosky et al., Do Data Breach Disclosure Laws Reduce Identity Theft? (Sept. 16, 2008) (unpublished manuscript, on file with author), *available at* http://ssrn.com/abstract=1268926.

166. Note the overall conclusion of Neil Robinson et al., Review of the European Data Protection Directive (2009) that

> as we move toward a globally networked society, the Directive as it stands will not suffice in the long term. While the widely applauded principles of the Directive will remain as a useful front-end, they will need to be supported by a harms-based back-end in order to cope with the growing challenge of globalisation and international data flows.

Id. at vii; *see also* F. FABBRINI ET AL., COMPARATIVE LEGAL STUDY ON ASSESSMENT OF DATA PROTECTION MEASURES AND RELEVANT INSTITUTIONS (EUI, 2009) (noting several deficiencies in compliance); *cf. supra* note 140 and accompanying text.

established could lead to future disadvantages, for example, when profile-based price discrimination is introduced.[167]

Second, there is the same potential disciplining effect resulting from awareness of being watched as in the previous power relations. As various authors have noted, "private entities are happily and busily creating their own independent Panopticons,"[168] and surreptitiously, "consumers are being disciplined *by consumption itself* to obey the rules, to be 'good' not because it is morally preferable to being 'bad' but because there is no conceivable alternative to being good, other than being put outside the reach of benefits."[169] The second and third dimensions of power (the indirect influencing of people's actions)[170] that are at play here surely call for reflection on the legal protection of consumers, since most consumer protection mechanisms focus on the exercise of the most visible first dimension of power (directly causing the consumer to do something which she would not otherwise do).

Before we take an integrated look at the three power relations we have studied, however, it is interesting to note that, perhaps more than in the previous power relations, the consumer domain itself shows signs of resistance against the panoptic gaze of e-businesses. Successful grassroots campaigns have fought many sometimes absurdly privacy-invasive applications proposed by companies, such as Intel's "Big Brother inside" chip,[171] Sony's rootkit,[172] information-hungry RFID chips,[173] NebuAd,[174] and

167. On price discrimination, see, for example, Rajiv Dewan et al., *Product Customization and Price Competition on the Internet*, 49 MGMT. SCI. 1055 (2003) (examining the effect of product customization on price in markets with monopolies and duopolies). While price discrimination based on an incorrect profile could equally benefit the consumer, from a Rawlsian perspective of fairness and consumer protection, the possible disadvantage of being offered a higher price based on incorrect data carries more weight than the possible advantage of being offered a lower price based on incorrect data.

168. Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 853 (2000).

169. REGINALD WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 142 (1999); *see also* Dholakia & Zwick, *supra* note 159, at 10 ("The superpanopticon erected by the new information entrepreneurs allows personal data to play a distinctive role in the modern STP (segmenting, targeting, and positioning) marketing process" and this "bestows consumer-friendly concepts like 'customization' and 'personalization' with the dark aura of totalitarian control."); Koops & Leenes, *supra* note 125, at 118, 129–32.

170. *See supra* Section II.A.

171. Intel's new Pentium III chip was proposed to include a unique Processor Serial Number, enabling identification of each and every single computer. Big Brother Inside, Latest News, April 28, 2000, http://bigbrotherinside.org/.

172. Sony's rootkit consisted of spyware on music CDs that was automatically installed on computers and created security vulnerabilities for the computers. *See* Wikipedia, Sony BMG CD Copy Protection Scandal, http://en.wikipedia.org/wiki/Sony_BMG_CD_copy_

Webwise.[175] An unorthodox, if perhaps rather desperate, anti-surveillance strategy could also be perceived in digital exhibitionism:

> [u]ltraexhibitionism, we argue, is not a negation of privacy but an attempt to *reclaim some control over the externalization of information*. As such, ultraexhibitionism is to be understood as an act of resistance against the surreptitious modes of profiling, categorization, and identity definition that are being performed *by others* on the consumer whenever he or she enters the electronic "consumptionscape."[176]

Thus, the active disclosure of large amounts of detailed personal information on the Internet could emerge as a new strategy of consumers to counter the risks of errors and panopticism associated with the increasing profiling power of businesses.

VI. THE IDENTITY OF THE CITIZEN–CONSUMER–EMPLOYEE

The previous Parts have discussed three distinct power relations involving different roles of individuals. Several similarities can be observed in the developments of the domains discussed, which suggest that certain general conclusions can be drawn on technology-related shifts in power relations and their consequences for legal protection.[177] Before drawing such conclusions, however, we must face a new issue that emerges from the discussion. Some shifts in power relations broaden or blur contexts, particularly with the creation and interconnection of public and private databases that cross the boundaries of law enforcement, employment, and commerce. This calls into question the sectoral approach to inequality compensation. Is it enough to protect individuals in their role as citizen, employee, and consumer, or should we also seek legal protection for

---

protection_scandal (last modified Feb. 5, 2010).

173. RFID chips are "smart" chips for wireless identification of objects at small distances, enabling for example tracing of consumer products. *See* CONSUMERS AGAINST SUPERMARKET PRIVACY INVASION & NUMBERING ET AL., RFID POSITION STATEMENT OF CONSUMER PRIVACY AND CIVIL LIBERTIES ORGANIZATIONS (2003), http://www.privacyrights.org/ar/RFIDposition.htm.

174. NebuAd was a company offering a service for behavioral advertising with ISPs transferring user communications to NebuAd for real-time profile-based advertising. Wikipedia, NebuAd, http://en.wikipedia.org/wiki/NebuAd (last modified May 20, 2010).

175. Webwise is a profile-based advertising system from Phorm, similar to NebuAd. *See* Antiphorm, http://www.antiphorm.co.uk/ (last visited Feb. 10, 2010); Wikipedia, Phorm, http://en.wikipedia.org/wiki/Phorm (last modified Nov. 13, 2009).

176. Dholakia & Zwick, *supra* note 159, at 13.

177. *See infra* Sections VII.A & VII.B.

individuals regardless of their role? To answer these questions, we need to broaden our view and look deeper into the identity of today's individuals.

This Part will start with a description of how identity construction takes place, in a context-dependent presentation of someone's self in her various roles in everyday life. The discussion will draw upon the findings of the previous Parts to argue that the shifts in power relations of the citizen–employee–consumer result in a mixing of contexts, which could well become responsible for a digital identity crisis. Moreover, another development affecting identity construction is taking place—panopticism. These insights in identity construction of today's individuals will subsequently be of use when overall conclusions are drawn on legal protection of weak parties in the next and final Part.

A. ROLE-PLAYING, IDENTITY, AND SELF-DEVELOPMENT

Until this point, we have encountered three characters in search of legal protection: the citizen, the employee, and the consumer. They are embodied in a single person, manifestations of an actor playing different roles in different contexts to which different areas of the law apply—constitutional and administrative law, labor law, and contract and tort law, respectively. I purposefully use the imagery of the stage here; Erving Goffman has shown how the presentation of the self in everyday life builds on the ability to set the stage that defines the situation in which others form opinions of oneself and to act a part that conveys the most favorable impressions of oneself.[178] The ability to influence the conduct of others by this role-playing and stage-setting is a crucial part of social life.[179]

Self-presentation is equally crucial for identity-building and self-development, since the sense of self develops according to how we perceive others to perceive us. We construct our identities by anticipating how others are profiling us.[180] For example, Johnny believes himself to be a cool guy, not because wearing Calvin Klein intrinsically makes him cool, but because Johnny thinks his peer group will think him cool when they see him wearing Calvin Klein underpants.

In power relations between A and B, the ability of B to control the presentation of self—and therefore construct an identity—is impaired, since it is usually A rather than B who sets the stage. This is why many legal mechanisms to protect weak parties aim at enhancing their ability to control the situation, by decreasing the information asymmetry, giving them access to

178. ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).
179. *Id.*
180. WP7, *supra* note 146, at 15–17.

mechanisms for redress, or increasing their ability to make autonomous choices. Data protection is often presented as informational self-determination: the ability of data subjects to control the dissemination of information about themselves.[181]

The process of identity construction is dynamic and time-dependent, building a continuously adaptive narrative of "who I am."[182] It is also context-specific; my sense of self is not a single, clearly definable "I," but a complex amalgam of different "mes," which come to the forefront in different settings.[183] Within the context of this Article, the fact that I am a researcher at the Tilburg Institute for Law, Technology, and Society is more relevant than my being a Dutch citizen or an online buyer of books, and consequently, I present more credentials relating to my scholarship than to my political inclinations or my customer profile at Amazon.[184] In other contexts, however, my role as a citizen or a consumer may be more prominent, and—just like my anticipation of the reactions to this Article influence my self-presentation and self-image as a scholar—my identity as a citizen or a consumer will be influenced by what happens to me, and by what I make happen, in those contexts.

These insights into role-playing and identity construction are presented here to illustrate a crucial point for this Article's theme. The legal protection of weak parties in power relations is defined by the roles these parties play, and these roles are played out in separate contexts regulated by separate areas of the law. However, having observed some shifts in power relations taking place that broaden or blur contexts, we should ask whether these contexts

---

181. See seminally, ALAN F. WESTIN, PRIVACY AND FREEDOM (1967), and in the European context the Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court], Dec. 15, 1983, 1 BvR 209 (F.R.G.), *available at* http://beck-online.beck.de/?vpath=bibdata%2fents%2flmrr%2f1983%2fcont%2fLMRR.1983.0056.htm. Whether data protection as embodied in the American fair information processing principles or the European Data Protection Directive actually effectuates informational self-determination is another matter. The competing interest of the free flow of information and services in the internal E.U. market have also set their stamp on data protection legislation, leaving the data subject with relatively toothless tools to control the flow of her personal data in today's information economy and database nations. *See supra* note 166.

182. WP7, *supra* note 146, at 15–17.

183. On the different narratives that can be told about one's life and how these narratives complicate the construction of a singular identity, see KAREL ČAPEK, AN ORDINARY LIFE (M. & R. Weatherall trans., 1936).

184. Admittedly, literature can teach important lessons about scholarly questions, so that my roles as a researcher and as a reader of fiction intermingle, making some of my Amazon profile shimmer through in this article. *See* JOHN GIBSON, FICTION AND THE WEAVE OF LIFE (2007); *cf.* ČAPEK, *supra* note 183.

are still sufficiently separate, or separable, to determine the role and consequent legal status of an individual in the information society.

B. A DIGITAL IDENTITY CRISIS?

The shifts in power relations in the case studies partly occur within each separate context. Both the strong and the weak parties have in some sense gained power in relation to the other. In fact, today the same person can play different roles on both sides of the power relation. The most notable of the dual roles is the "prosumer," a person who is a consumer acting as a producer.[185] This also occurs in the rise of citizens participating in public policy-making[186] and of the self-employed worker. Some individuals, but by no means all, thus gather experience playing the role of the traditionally strong party on some occasions, which may help them when they act in their role as the traditionally weak party in other situations.

However, the shifts in power relations also have effects across contexts. In today's technology-mediated world, the person enacting citizenship, employeeship, and consumption is becoming a digital persona living in a myriad of databases, who may have less control over the specific role she is playing in different contexts. The labor context extends to non-labor time and space, where private activities may be monitored by employers enforcing their company policy of having "good" employees.[187] The consumer is digitized into interesting information segments that are distributed across networks and used to build profiles.[188] Citizens' activities are recorded and stored in databases regardless of whether there is a preexisting suspicion that they engage in criminal acts. Frequently, these databases are controlled by private parties such as telecom providers or airline carriers. In this way, private sector architectures for doing business are being adapted to meet public policy goals of crime and terrorism fighting.[189] Internet Service

---

185. *See* ALVIN TOFFLER, THE THIRD WAVE 282–305 (1980).

186. On participatory governance, see, for example Cary Coglianese, *Citizen Participation in Rulemaking: Past, Present, and Future*, 55 DUKE L.J. 943 (2006).

187. *See supra* Section IV.C.

188. Dholakia and Zwick state that

> With privacy dispossession, the consumer most significantly loses the power over his or her *representation* as consumer in the market. Someone else's image of what the consumer *might be* takes on a *real* existence. These synthesized representations of the consumer "self" are being distributed through information entrepreneurs to the databases of the world.

Dholakia & Zwick, *supra* note 159, at 17; *see also supra* Section V.C.

189. *See supra* Section III.D.

Providers are increasingly harnessed as nodal points to monitor and intervene in the enforcement of private and public rights and duties.[190]

In this world of interconnected or interconnectable databases, digital representation is slowly but surely overtaking physical presentation in face-to-face contacts: the "data double is more real tha[n] the person behind it."[191] The digital persona of the citizen–employee–consumer increasingly functions as her interface in the power relations with the government–employer–producer, resulting in decisions based on data stored in databases.[192] These databases, however, generally do not intrinsically retain the original context of the data stored in them. When function creep leads to data being exchanged and used in other contexts, the primary context often is lost. The power and attractiveness of databases lie not only in their persistence and comprehensiveness, but also in their multifunctionality. The logic of a world that thrives on databases is therefore at odds with purpose specification and use limitation, two important principles of the data protection framework. Today, I seriously doubt that purpose specification and use limitation continue to play a substantial role in practice.

The transformation of a person playing different roles in context-rich, face-to-face situations into a person interacting in different power relations through the interface of a context-poor but potentially information-rich digital persona has important implications for self-presentation and identity construction.[193] Goffman describes how roles are typically played before the same or similar audiences:

---

190. Koops & Leenes, *supra* note 125, at 118 ("An interesting aspect of this Internet Panopticon is that the state shifts the responsibility of enforcement to entities in the private sector, such as Internet service providers (ISPs)."); *see also* EGBERT DOMMERING, GEVANGEN IN DE WAARNEMING. HOE DE BURGER DE COMMUNICATIEMIDDELEN OVERNAM EN ZELF OOK DE BEWAKING GING VERZORGEN (2008); Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. Rev. 653 (2003).

191. Maria Los, *Looking Into the Future: Surveillance, Globalization and the Totalitarian Potential*, *in* THEORIZING SURVEILLANCE 69, 86 (David Lyon ed., 2006).

192. SOLOVE, *supra* note 66; *see* Roger Clarke, *The Digital Persona and Its Application to Data Surveillance*, 10 INFO. SOC'Y 77 (1994); Los, *supra* note 191, at 87 (noting that "both actuarial calculations and data-matching procedures constantly produce real consequences for individuals represented by their ersatz doubles").

193. Los, *supra* note 191, at 78. Los notes that

> the fragmented, decontextualized information, collected for many specific purposes, may acquire a multitude of completely different meanings depending on its particular compilation, re-contextualization and application. As well, because of the ramified nature of data neworks, it appears practically impossible to correct erroneous or twisted information. In this context, the notion of biographical truth loses any meaning.

> [d]efining social role as the enactment of rights and duties attached to a given status, we can say that a social role will involve one or more parts and that each of these different parts may be presented by the performer on a series of occasions to the *same kinds of audience* or to an *audience of the same persons*.[194]

How can a person present herself—or her self—as a digital person when it is almost impossible to know from the outset what her audience will be? Which social role can or should she play in her guise as a digital persona performing multiple functions in public–private database conglomerations? And can the presentation of the self be at all controlled by the person when the presentation is digitized in databases? Altogether, the shifts in power relations of the citizen–employee–consumer and the associated mixing of contexts could well become responsible for a digital identity crisis.[195]

C. PANOPTICISM AND NORMALIZED IDENTITY

A digital identity crisis is, however, not the necessary outcome of the shifts in power relations studied. Besides the shattering of the person across databases, a second development is taking place: panopticism.[196] In all three power relations, to greater or lesser degrees, this mechanism at play is distinguished. The citizen–employee–consumer is increasingly being watched in and across the different contexts in which she acts. The awareness that any activity may be observed has a potentially self-disciplining effect, through which the person embraces society's paradigm of normality and starts to behave accordingly.[197]

Panopticism also affects identity construction. Profiling is a key technology that causes shifts in all three power relations studied, because it is associated with panopticism and may, through panoptic logic, affect the freedom of persons to construct their identities.[198] Through the double

---

Id.

194. GOFFMAN, *supra* note 178, at 16 (emphasis added).

195. *Cf.* Los, *supra* note 191, at 85 ("The new logic of late-modern surveillance, typified by the data double, dehumanization of freedom and de-socialized criteria of sorting, suggests a special form of biographical uprooting, whereby for many people a caring relationship with their peripatetic, de-contextualized virtual double(s) is likely to become a major preoccupation.").

196. *See supra* Section II.A.

197. It should be noted that awareness of the average person of being watched through data surveillance may currently be fairly low. It is expected to rise, however, with the increase of personal experiences, media stories, and growing intrusiveness of surveillance practices. *See* Los, *supra* note 191, at 77, 80–81.

198. *See supra* note 137 and surrounding text; *see also* Hildebrandt, *supra* note 68, at 305–11.

anticipation that is at work in identity building, the panoptic embracing of the "system's" paradigm of normality has a major impact on the resulting identity. The digital personae that represent the person in today's database-based power relations *constitute* their identity as much as they are *constituted by* the person's self-presentation in everyday life. Where panopticism is at work, there is little difference between an imposed persona (i.e., the representing profile imposed by a counter-party) and a projected persona (i.e., the self-representing profile controlled by the person herself)[199]: both reflect the prevalent paradigm of how someone is supposed to behave.[200]

Here, we can observe the third dimension of power at work: the socially structured and culturally patterned practices of institutions of government, labor, and consumption reinforce existing imbalances in the power relations. The weak parties see no other option but to embrace their (self-)imposed normalized digital personae as constituting who they are, rather than challenging their digital personae to represent the persons they want to be.

VII. CONCLUSIONS AND OUTLOOK

After the tour d'horizon of developments in the power relations between government–citizen, employer–employee, and business–consumer and the integrated vision of the identity of today's citizen–employee–consumer, it is time to return to the questions posed at the outset. What technology-related shifts occur in power relations in the domains of government, labor, and commerce? And what are the consequences of these shifts for the legal protection of weak parties, in particular, for existing mechanisms of inequality compensation in the associated legal domains?

This Part begins with a summary of the shifts in power relations discussed previously. Next, a discussion follows of the consequences for legal protection: first, within the realms of criminal, labor, and consumer law, and subsequently, beyond context-specific forms of inequality compensation. The analysis highlights the importance of having a comprehensive data protection framework. This Article concludes with a sketch of two alternative directions for such a framework to protect citizens in today's cross-context database society.

---

199. Clarke, *supra* note 192.

200. *Cf.* MANUEL CASTELLS, THE POWER OF IDENTITY 7 (1997) ("Although . . . identities can also be originated from dominant institutions, they become identities only when and if social actors internalize them, and construct their meaning around this internalization."). Panopticism precisely has such an internalizing effect. *See also* Los, *supra* note 191.

A. SHIFTS IN POWER RELATIONS

With the development of new technologies—in particular ICT, but also genetic applications—power relations shift in various ways. Most shifts relate to an increase in information: both the traditionally strong parties (i.e., governments, employers, business) and the traditionally weak parties (i.e., citizens, employees, consumers) use ICT, and sometimes DNA techniques, to improve their information position. These shifts do not counterbalance each other. Rather, they are asymmetrical: they involve different types of information, different situations, and—particularly in the government context, but probably also in commerce—different sub-groups that are affected. Although the weak parties can use their improved information position to resist or bypass the power exercise of the strong parties, in many cases, the strong parties can use their improved information position to exercise power even more strongly and in different ways.

Particularly in the government and employment context, the empowerment of the strong party fundamentally affects the character and scope of the power relation. Criminal law is shifting from a reactive, incidental, last-resort mechanism to a preventative, comprehensive, and primary regulatory mechanism. Since this reshaping of criminal law involves massive-scale data collection, storage, and profiling of unsuspected citizens, the nature of the government–citizen relationship is slowly changing. Citizens are treated less as prima facie trustworthy subjects and more as prima facie risk objects.

A similar development, although much smaller in scale and scope, can be seen in the employment context, where employers are now monitoring their employees on a routine basis and also increasingly in off-duty situations. A crucial consequence of the changed nature of these power relations is that contexts are broadened and become intertwined: the data involved in the "risk management" of citizens and employees are stored in interconnected or interconnectable databases. Here, the commerce sector also enters the picture, since several of these databases are outsourced to third parties. These third-party information brokers or intermediaries then fill or merge the data of such databases with that of the commercial databases. Thus, database and profiling technologies are facilitating the rise of comprehensive monitoring systems that move between and across different contexts.

An important feature of the technology-facilitated changes in the nature of power relations is the rise of "governing through crime," which implies that the contexts of crime (and criminal law) and other sectors of society (and their associated areas of law) are increasingly overlapping. Particularly in the United States, but also visible on a smaller scale in the Netherlands, many

types of relationships are increasingly cast in risk discourse and governed by mechanisms derived from or based in criminal law. These mechanisms include, for example, crime language, offender statistics, and sanctioning policies.[201] Many common spaces—schools, the family, the workplace—are adopting "practices suggestive of the penal aspects of criminal justice."[202] For example, the U.S. Safe Schools Act of 1994 created a "national model of crime governance for schools," encompassing zero-tolerance policies, disciplinary violations categorized as quasi-crimes, in-school detention systems, and data collection systems for (quasi-)crime monitoring.[203] In divorce cases, allegations of crimes committed by the partner have emerged as a primary argument in contested child custody and property distribution proceedings.[204] The Anti-Drug Abuse Act of 1988 comprises a "one strike and you're out" standard to evict tenants from public housing when she or "any guest or other person under the tenant's control" commits a drug-related offense on- or off-premises.[205] It is a strict liability standard that would permit a landlord to evict a mother for drugs her daughter possessed.[206] The "governance through crime" mechanism here is that the "exclusionary power associated with criminal designation [is also used] to accomplish other organizational goals (like ridding schools of poor test takers or ridding public housing of waiting lists) . . . ."[207]

In this altering landscape of context-crossing power relations, two overarching trends stand out: the use of digital personae as a substitute for the physical persons of the weak parties in power relations, and the creation of panoptic risk-governing architectures that have a potentially self-disciplining effect on the weak parties. Some individuals from the category of traditionally weak parties may use the new technological opportunities to effectively resist the power exercised by the traditionally strong party. However, the combination of these trends implies that many, if not most, individuals within the weak-party categories face new, difficult to counter, and more diffuse, context-crossing, and subtle forms of power exercise by the strong parties.

---

201. Simon, *supra* note 69, at 221.

202. *Id.*

203. *Id.* at 214–31. Illustrative is the Ruffner Middle School (Norfolk, Virginia) mandatory uniform policy. "Students who come to school without a uniform are subject to in-school detention," which is reported as successful in improving student behavior: "throwing objects is down 68 percent and fighting has decreased by 38 percent." *Id.* at 225.

204. *Id.* at 192.

205. *Id.* at 194–95.

206. *Id.*

207. *Id.*

B. CONSEQUENCES OF LEGAL PROTECTION

The shifts in power relations raise questions about the ability of current mechanisms to compensate weak parties for structural inequalities. The case studies in this Article have uncovered insufficiencies or inadequacies in current legal protection. Each legal field—criminal, constitutional, administrative, labor, and consumer law—requires adaptation to meet the new reality. This has already partly been achieved, for example, with the introduction of consumer protection rules in e-commerce legislation and the creation of guidelines for responsible monitoring of employees.[208]

However, much remains to be updated. For example, adequate protection against the use of new applications, such as familial DNA searching or behavioral advertising, must be devised. This is a matter of course: the law usually lags behind technological developments, and it is unsurprising that legal-protection mechanisms will eventually be adapted or created for such new developments.

The U.S. legal system is arguably better equipped than the Dutch legal system to achieve this because its reliance on case-law besides statutory law ensures that it can relatively swiftly adapt to new technological realities. Constitutional review allows modern-day re-interpretation of age-old constitutional protection provisions.[209] Furthermore, its statutes frequently contain open norms that can be flexibly interpreted by the courts,[210] and its greater reliance on the market also allows for more flexibility.

Nevertheless, the flexibility and use of open, re-interpretable norms in the U.S. approach also have drawbacks for legal protection, since the legal norms can easily and docilely follow technological and market developments rather than actively shape these developments. For example, this is visible in

---

208. *See supra* notes 113–14, 153–56 and accompanying text.

209. In the Netherlands, constitutional review by the courts is unconstitutional. GRONDWET VOOR HET KONINKRIJK DER NEDERLANDEN [GW.] [Constitution] art. 120 (Neth.). A Bill is pending to amend this (Kamerstukken II, 2001–2002, 28 331 (Neth.)), but it is dubious whether this Bill will be adopted in the foreseeable future. The Dutch constitutional system is therefore much more rigid, leading to technology-specific constitutional provisions, like the freedom of the printing press and the secrecy of telegraphy, becoming outdated without legal certainty with respect to "new" technologies like the Internet. For a comparison of the Dutch and American approaches to "digital constitutional rights," see Bert-Jaap Koops & Marga Groothuis, *Constitutional Rights and New Techonologies in the Netherlands*, *in* CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES: A COMPARATIVE STUDY (R. Leenes et al. eds., 2008) and Susan W. Brenner, *Constitutional Rights and New Technologies in the United States*, *in* CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES: A COMPARATIVE STUDY (R. Leenes et al. eds., 2008).

210. For example, in the requirements for interceptability of telecommunications, see *supra* Section III.B.

the erosion of privacy protection through the technology-facilitated erosion of reasonable expectations of privacy.[211] Technology and the market are not usually allies of weak parties, and hence, the law should have firm mechanisms in place when it is to provide protection to weak parties in the face of technology-related shifts in power relations. It remains to be seen whether, in general, the more flexible and responsive, but also more fluid and market-oriented character of the U.S. approach is better able to meet the challenges of providing legal protection in power relations than the slower and more rigid, but also more principled and paternal character of the Dutch approach.

Regardless of the specifics of legal systems and concrete changes that may need to be made in specific areas of law, two general conclusions can be drawn on legal protection of weak parties. One problem resides in the shift from a reactive, incident-driven approach to a preventative, comprehensive approach. It is most obvious in criminal justice, but it is also visible in other contexts where risk governance is gaining ground. Legal protection of weak parties in a reactive, incident-driven system tends to focus on preventing or redressing grave errors that may incidentally occur, for example, sending an innocent person to jail or having an ignorant consumer declared bankrupt after being lured into buying a high-risk financial product. When the system becomes preventative and comprehensive, however, the vulnerability does not lie solely in incidental major errors or injustices, but in frequent minor errors or injustices. Examples include wrongly blacklisted passengers being detained at airports for a few hours, employees forced to explain with occasional embarrassment what they (or their cars) were doing at dubious locations, children's rights organizations finding their websites blocked by overzealous child pornography filtering systems. Such relatively small inconveniences, with minor damage, will not be set right by legal-protection mechanisms based on the old paradigm of addressing incidental grave errors. The law should therefore be supplemented with new forms of legal protection that can prevent or redress adequately the overall functioning of comprehensive risk-governing systems. This means introducing more administrative and accountancy-type checks and balances, such as regular audits by independent supervisors monitoring the fairness of policies and practices, low-threshold complaint mechanisms with teeth to call the strong

211. Koops & Leenes, *supra* note 125 (finding that technology does not incorporate privacy norms and erodes reasonable expectations of privacy); Phillips, *supra* note 49, at 59 ("This reliance on the market as a policy mechanism for privacy protection reinforces and exacerbates unequal power relations between employers and employees.").

parties to order, and liberal compensation mechanisms for people suffering inconveniences and smaller injustices.[212]

A second overarching problem that needs to be addressed is the gap between law in the books and law in action. This problem occurs most notably in data protection but also in employment law (e.g., the difficulty of achieving redress) and consumer law (e.g., the lack of individual access to justice through dispersion of damage). The gaps in data protection and privacy law are systemic, and in the era of databases, profiling, ubiquitous computing, and Ambient Intelligence,[213] law in the books has reached the limits of its powers. As a result, legal protection should not only be articulated in written law, but also in the socio-technical infrastructure itself. Both PETs and transparency enhancing technologies (TETs) must be developed that embed legal rules in present and future ubiquitous technologies.[214] The same may well apply to other areas of legal protection, including legal mechanisms in labor and consumer law, which are difficult to enforce in today's technology-pervaded world. "Code as law" will be required to supplement law in the books if weak parties are to be effectively protected.[215]

C. BEYOND CONTEXT-SPECIFIC INEQUALITY COMPENSATION

It is insufficient to adapt legal protection, as outlined in the previous Section, only within each specific area of law where inequality-compensating protection mechanisms are found. The search for legal protection of weak parties should not be restricted to the specific context of their concrete role as citizen, employee, or consumer. On the contrary, the key challenge of updating inequality compensation in light of technology-related shifts in power relations lies in finding ways to empower individuals with means to develop themselves and to construct their identities in a technology-mediated

212. G.G. Fuster & P. De Hert, *PNR and Compensation: How to Bring Back the Proportionality Criterion*, *in* ARE YOU WHO YOU SAY YOU ARE? THE EU AND BIOMETRIC BORDERS 101, 108 (2007) ("The [compensation] mechanisms as envisaged in this paper will offer potentially many more benefits than mere individual redress. Their efficiency in generating collective benefits, however, relies ultimately on the generosity of the compensation. . . ."); Koops, *supra* note 64.

213. Ambient Intelligence refers to the concept of sensor-equipped environments that respond in real-time to the people moving around in them. *See generally* THE NEW EVERYDAY: VIEWS ON AMBIENT INTELLIGENCE (Emile Aarts & Stefano Marzano eds., 2003) (discussing Ambient Intelligence, its potential, implications and potential problems).

214. M. Hildebrandt & Bert-Jaap Koops, *The Challenges of Ambient Law and Legal Protection in the Profiling Era*, 73 MOD. L. REV. 428 (2010).

215. Employing "code as law" is easier said than done if it is to be both effective and legitimate. *See id.* This is one of the major challenges for future interdisciplinary research. *Id.*

world that obfuscates the audiences for which they play their different roles as citizens, employees, and consumers.

The main trends in the shifts in power relations are the use of context-poor digital personae and the creation of panoptic monitoring architectures.[216] The resulting vulnerabilities are increased risks of errors in interpretation, as well as a normalizing, self-disciplining effect of the panoptic architectures on individuals' behavior and identity construction. Both of these trends and vulnerabilities are related to the fact that myriads of personal data are stored and processed in diverse power relations, and possibly exchanged across contexts. The key issue is who is allowed to process which data for which purposes and under which conditions. In other words, data protection turns out to be the major mechanism that deals with the key issue in reducing vulnerabilities emerging through the shifts in power relations. If people are to be protected against abuses of power in the era of databases and profiling, then some form of data protection is crucial. Furthermore, this data protection should be generic rather than context-specific because the audiences of digital personae are far less clearly distinguishable than the audiences for physical, role-playing persons.

The European, general approach to data protection is more adequate in that respect than the context-specific, piecemeal approach of the United States, but the comprehensive European approach to data protection also faces considerable challenges. For instance, as discussed above, the European approach must deal with the sustainability of the purpose-specification and use-limitation principles in a database-pervaded world,[217] the gap between law in the books and law in action, and the consequent need to build in PETs and TETs in socio-technical architectures.[218]

Can a comprehensive data protection framework actually meet all these challenges, in order to provide cross-context inequality compensation to the citizen–employee–consumer, as represented by her proxy, the digital persona? In other words, can data protection be made to empower people to control their digital personae to such an extent that they can resist the abuse of power by different strong parties in diverse and opaque situations? In theory, it can. *How* it can achieve this, however, is a matter of debate. The literature seems to suggest two radically different directions for empowering persons.

216. *See supra* Section VII.A.
217. *Supra* Section VI.B.
218. *Supra* Section VII.B.

D. TWO DIRECTIONS TO EMPOWER PERSONS

1. The Orthodox View: Resistance by Data Limitation and User Control

The first way in which persons can be empowered to resist the exercise of power by diverse strong parties in the face of ubiquitous databases and profiling, is to make the current data protection framework more effective. This approach uses a two prong strategy to empower data subjects to gain and retain a substantial level of control over their personal data in the world's myriad databases, as well as over their digital personae. The first prong requires that purpose-specification and use-limitation principles remain cornerstones of data protection, and hence, limits are set on who can access and process which personal data for which purposes. To meet the realities of today's database world, however, these limits may be less strict in terms of preventing data processing. This is then compensated by stronger requirements for making the processing, particularly if used for other purposes, more transparent to and challengeable by data subjects. The other prong is that these limits and requirements are to be enforced more effectively in practice than is the case today, particularly by using PETs and TETs.

Advocates for this approach are typically the data-protection community—a loose network of professionals and scholars aiming to develop and preserve data protection, including Data Protection Authorities and Information Commissioners, privacy advocates, and experts in the field of data security.[219] This approach builds on Nissenbaum's notion of "contextual integrity," which presents a context-sensitive "justificatory framework for prescribing specific restrictions on collection, use, and dissemination of information about people."[220] This approach explores possibilities to achieve "privacy in the clouds," where cloud computing and Web 2.0 call for identity-management systems that are under the control of users; these possibilities include technical and organizational solutions, such as open-source software, federated identity management, multiple and partial identities, audit tools, and data-centered or "sticky" policies.[221] The vision of

---

219. The latter is exemplified in the title of the German journal *Datenschutz und Datensichterheit* [Data Protection and Data Security], the authorship and readership of which constitute a significant part of the continental data protection community.

220. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 155 (2004); *see also* Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1051 (2009) (arguing that even when people voluntarily disclose personal information on the web such as on social network sites, a reasonable expectation of privacy remains as long as the information remains inside the network in which it was disclosed).

221. Ann Cavoukian, *Privacy in the Clouds*, 1 IDENTITY INFO. SOC'Y 89 (2008); *see also* Jan

Ambient Intelligence, in this approach, is to be realized by architecture-embedded Ambient Law in the form of PETs and TETs.[222] In short, this approach holds that by harnessing technology through technology, a new and more effective generation of context-sensitive data protection can be achieved.

2. *The Radical View: Resistance by Data Proliferation and Looking in Return*

The second approach to empowerment is more unorthodox and radically different. The power of panoptic architectures can be resisted, in this approach, by beating the observers at their own game. This resistance can take a number of manifestations. For example, using the method of the "Jam Echelon Day," in which the Anglo-Saxon intelligence snooping network Echelon was to be clogged by including in each e-mail message a signature with fifty "red-flag" words,[223] panoptic observers can be overwhelmed by creating such enormous haystacks of personal data that the needles are hopelessly lost. Another manifestation of this type of resistance is exhibitionism—disclosing a complete digital persona online that is fully visible in order to preempt others from constructing a digital persona for you. By anticipating imposed personae and exhibiting "adult" versions of their projected persona, people can retain a sense of control in the construction of their identity.[224]

Unorthodox as this approach may be, it aligns with other developments in the network society, such as crowdsourcing, viral marketing, free

---

Camenisch et al., Privacy and Identity Management for Everyone, *in* PROCEEDINGS OF THE 2005 WORKSHOP ON DIGITAL IDENTITY MANAGEMENT 20–27 (2005); Marco Casassa Mont et al., *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services*, *in* PROCEEDINGS OF THE 14TH INTERNATIONAL WORKSHOP ON DATABASE AND EXPERT SYSTEMS APPLICATIONS 377 (2003); PRIME-Privacy-Enhanced Identity Management in Europe, http://www.prime-project.eu (last visited Sept. 25, 2009).

222. Mireille Hildebrandt, *A Vision of Ambient Law*, *in* REGULATING TECHNOLOGIES: LEGAL FUTURES, REGULATORY FRAMES AND TECHNOLOGICAL FIXES 175, 188–89 (Roger Brownsword & Karen Yeung eds., 2008).

223. An example of an Echelon-jam-generated e-mail signature is: "ATF DOD WACO RUBY RIDGE OKC OKLAHOMA CITY MILITIA GUN HANDGUN MILGOV ASSAULT RIFLE TERRORISM BOMB DRUG KORESH PROMIS MOSSAD NASA MI5 ONI CID AK47 M16 C4 MALCOLM X REVOLUTION CHEROKEE HILLARY BILL CLINTON GORE GEORGE BUSH WACKENHUT TERRORIST." Chris Oakes, *Monitor This, Echelon*, WIRED, Oct. 22, 1999, http://www.wired.com/print/politics/law/news/1999/10/32039/.

224. Dholakia & Zwick, *supra* note 159, at 1 (noting that "exhibitionism and voyeurism seem to offer new tools for consumer resistance against the electronic surveillance systems in networked markets and are inextricably interwoven with consumers' desire for control over their information"); *see also supra* note 176 and accompanying text.

distribution of goods as a new business model, and a "pirate's" approach to information dissemination,[225] all of which involve an extreme proliferation of data and a re-evaluation of the value attached to those data.

Besides data proliferation, the most pertinent manifestation of this type of resistance is the vision of David Brin, who proposes the strategy of looking in return.[226] In Brin's view, checks and balances in a panoptic surveillance society are to be found in monitoring the monitors, not only by independent supervisors, but also and more importantly, by the people monitored: "we may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction."[227] By increasing transparency on all sides, a bottom-up coalition of amateur watchers will scrutinize the monitoring practices of the powerful: "the cameras *are* coming. You can rail against them, shaking your fist in futile rage at all the hovering lenses. Or you can join a committee of six billion neighbors to control the pesky things, making each one an extension of your eyes."[228] In this radical view, the glaring light of ubiquitous transparency is not incompatible with privacy; on the contrary, it safeguards privacy by its unique power to hold accountable those who violate privacy.[229] The power of knowledge may be wielded by data-collecting, strong parties, but abuse of power will immediately be brought to light by the power of numbers of weak parties who can scrutinize all the strong parties' actions.

E. CONCLUSION: NO MIDDLE WAY

This Article argues that technology-related shifts in power relations call for revision of the legal protection of weak parties, in particular, of mechanisms of inequality compensation. Part of this should be achieved by updating existing mechanisms in the associated legal domains, by critically reviewing existing provisions in criminal, administrative, labor, and consumer

225. *See, e.g.*, CHRIS ANDERSON, FREE: THE FUTURE OF A RADICAL PRICE 3 (2009) (discussing a new business model in which many people are "making lots of money charging nothing"); CHARLES LEADBEATER & PAUL MILLER, THE PRO-AM REVOLUTION: HOW ENTHUSIASTS ARE CHANGING OUR SOCIETY AND ECONOMY (2004) (discussing the counter-trend of Pro-Ams, "innovative, committed and networked amateurs working to professional standards," and their impact on society); MATT MASON, THE PIRATE'S DILEMMA: HOW YOUTH CULTURE IS REINVENTING CAPITALISM (2008) (describing how youth culture and trends have influenced society).

226. DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998).

227. *Id.* at 23.

228. *Id.* at 333.

229. *Id.* at 334.

law, to assess their ability to protect weak parties in light of shifts in power relations that empower the strong party, particularly when power is exercised in new ways.[230] However, sector-specific legal protection is not enough. We also need a comprehensive approach to protect individuals in a world where they interact with different strong parties through digital personae across contexts and in pervasively monitoring architectures. Such a comprehensive approach is most likely to be found in data protection: enforceable rules that regulate who can process which data for which purposes under which conditions.

However, it is unclear how empowerment of data subjects can best be achieved to meet the reality of today's database and profiling era. The dominant, orthodox strand in the literature favors the current European approach to data protection, focusing on data limitation and user control, and suggesting a concerted attempt to make this work in practice by implementing context-sensitive PETs and TETs. In contrast, a subsidiary, radical strand in the literature favors user-generated data maximization and counter-surveillance strategies based on transparency to resist the exercise of panoptic power.

Both directions for the next generation of data-protection frameworks have potential, and either will be a challenge to achieve. However, there is no middle path: the approaches of data limitation and data proliferation are incompatible with one another. We will have to choose between the orthodox and the radical approach. And while the debate continues, digital personae and panoptic architectures will continue to proliferate, playing into the hands of the powerful, and the citizen–employee–consumer of the database era will face an ever harder job to resist the exercise of those powers. A consistent approach to achieve effective data protection must be decided upon soon.

If the orthodox way does not prove successful in the coming years, then, perhaps, we should collectively shift to the radical way.

VIII. POSTSCRIPT: UMBERTO ECO'S ANOPTICON

The radical way will, like all radical suggestions, seem far-fetched and fraught with questions of feasibility. I will leave aside discussing these questions here, as they require considerable further research, and end instead with a visionary metaphor for the radical way, which can serve as a welcome

230. *See supra* Section VII.B.

contribution to the post-Foucauldian literature on panopticism and how to resist it: Umberto Eco's Anopticon.[231]

The Anopticon is a hexagonal building which effectuates "the principle of 'being able to be seen by everyone without seeing anyone.' "[232] The Anopticon's subject is a prison guard who lives in a closed, central hexagonal room, illuminated by a few conical embrasures which allow some light to shine through from above, but which do not permit the prison guard to see anything other than a small circular portion of sky. Around the prison guard's room are the prison's corridors where the prisoners can walk around freely.

From these corridors encircling the central room, the prisoners can watch the prison guard through conical embrasures, in such a way that the prison guard can not know when he is being observed, nor by whom. In fact,

> [t]he Anopticon does not allow the prison guard to have any control over the rest of the prison: he can not surveil the prisoners, he can not prevent their escape, he can not even know if there are any prisoners left nor whether anyone is watching him, and, supposing that someone were watching him, the prison guard is not capable of knowing whether it is a prisoner or an occasional visitor of this *machine-à-laisser-faire* (see also the married machines and *The virgin dressed by her other spouses*).[233]

As in the radical view of a maximally transparent society, Umberto Eco's Anopticon provides a new answer to the traditional question "Quis custodiet custodes?" It is we, the watched, who should watch the watchers.

231. Umberto Eco, *L'Anopticon*, *in* IL SECONDO DIARIO MINIMO 176 (1992).

232. *Id.* (translation by Bert-Jaap Koops).

233. *Id.* (translation by Bert-Jaap Koops). *The virgin dressed by her other spouses* is an inverse reference to Marcel Duchamp, *The Bride Stripped Bare by Her Bachelors, Even (The Large Glass)* (sculpture) (1923), which recalls associations of the work's machine-like appearance and of its Panopticon-suggestive nickname, "The Large Glass."